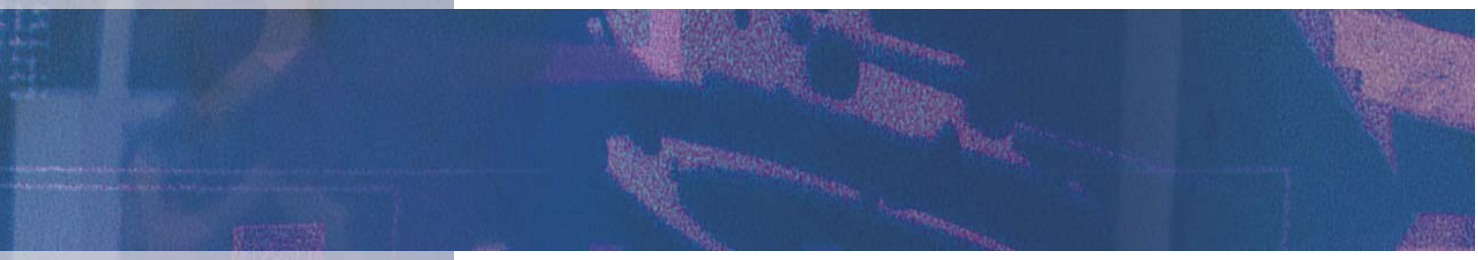
SOPHOS



sophos anti-virus

Windows 95/98/Me

User manual

For network and single users

Copyright © 2002 by Sophos Plc

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior permission in writing of the copyright owner.

Any name should be assumed to be a trademark unless stated otherwise. *InterCheck* and *Sophos* are registered trademarks of Sophos Plc.

Technical support

UK (24 hours):	(+44) 1235 559933 support@sophos.com
USA:	(+1) 888 767 4679 supportus@sophos.com
Australia (24 hours):	(+61) 2 9409 9111 support@sophos.com.au
France:	(+33) 1 41 99 94 20 support@sophos.fr
Germany (24 hours):	(+49) 6136 91193 support@sophos.de
Japan (24 hours):	(+81) 45 348 8400 support@sophos.co.jp
Singapore:	(+65) 6776 7467 supportasia@sophos.com

Contents

About Sophos Anti-Virus for Windows 95/98/Me 5

Installation

1 About installation 10

2 Creating the Windows 95/98/Me CID 11

3 Installing Sophos Anti-Virus on the workstations 20

4 Testing Sophos Anti-Virus on Windows 95/98/Me 24

Using Sophos Anti-Virus

5 Using the Sophos Anti-Virus window 26

6 Using InterCheck Monitor 34

7 Disinfection 35

8 On-screen log messages 41

Configuration

9 Configuring immediate and scheduled scanning 48

10 Configuring InterCheck 56

11 Alerts configuration options 64

12 Global configuration options 69

13 Sophos Anti-Virus command line qualifiers 74

Updates

14 Performing a monthly update 76

15 Performing an emergency update 79

Troubleshooting

16 Troubleshooting 84

Glossary and index

Glossary 90

Index 94

About Sophos Anti-Virus for Windows 95/98/Me

This section describes Sophos Anti-Virus and gives an overview of how you install and update it on Windows 95/98/Me workstations on a network.

What is Sophos Anti-Virus?

Sophos Anti-Virus is software that can

- detect viruses
- report virus finds to a central location (i.e. the server)
- disinfect viruses.

Sophos Anti-Virus can run on individual computers or entire networks.

How is Sophos Anti-Virus installed?

The following is a brief description of how you install Sophos Anti-Virus on Windows 95/98/Me computers on a network. This user manual includes a full explanation of every Windows 95/98/Me installation option (see section 1).

For a list of cross-references to installation guides that contain the ***recommended*** installation procedures for Windows 95/98/Me workstations, see section 1.

1. **Install Sophos Anti-Virus on the server.**

   For instructions, refer to the Sophos Anti-Virus user manual for the server platform.

2. **Create a central installation directory (CID) for Windows 95/98/Me (section 2).**

   The CID should be installed on the Windows NT, Windows 2000, NetWare or Unix server. When you update Sophos Anti-Virus for Windows 95/98/Me, it will only be necessary to update this CID.

3. **Install Sophos Anti-Virus on the workstations (section 3).**

   The easiest way to install Sophos Anti-Virus on the workstations is to use the login script. Alternatively, you can install it on each workstation individually.

   You should always install InterCheck Client on workstations. InterCheck Client checks files for viruses as they are accessed by the computer, and denies access if they are found to be infected. See section 5.4 for more information about InterCheck.

How is Sophos Anti-Virus updated?

Sophos Anti-Virus can only detect and disinfect viruses known to Sophos before each version is compiled. You must therefore update your installation frequently to ensure it is capable of recognising the latest viruses. Update Sophos Anti-Virus at the following times:

Every month (section 14)

Every month, Sophos releases a new version of Sophos Anti-Virus on CD and on the website. New versions contain new functionality, as well as the capability to detect the latest viruses. You must update your Sophos Anti-Virus CIDs as soon as you receive the new CD. The computers on the network update automatically from the updated CID.

Remember that you must update Sophos Anti-Virus for each platform (i.e. if you have both Windows NT/2000/XP and Windows 95/98/Me workstations, you must update both CIDs).

When there is a new virus (section 15)

When Sophos identifies a new virus, it issues a virus identity file (IDE), a type of file that enables Sophos Anti-Virus to detect that virus. Download IDEs from the Sophos website (www.sophos.com/downloads/ide) and save them in each of your Sophos Anti-Virus CIDs.

To receive email notifications about IDEs and other alerts, register at www.sophos.com/virusinfo/notifications.

What if Sophos Anti-Virus finds a virus?

Isolate the infected computer from the network and internet and write down the name of the virus (this is displayed in the virus alert message box and in the on-screen log in the **Sophos Anti-Virus** window). Look up the analysis for the virus on the Sophos website to find out what course of action to take, or contact Sophos technical support.

See section 7 for general information about automatic disinfection.

How else can you protect your computer or network from viruses?

The book *Computer viruses demystified* (enclosed with your first Sophos CD) describes many common types of virus and what you can do to avoid being infected by them. If you do not have a copy, a PDF version is available from both the Sophos website and the Sophos CD.

You should also:

- Investigate potential loopholes such as unpatched servers, which may allow viruses into your organisation. Install all relevant software patches as soon as they become available. You can keep track of newly available software patches at www.sophos.com/support/news.
- Advise your users not to run executables they receive as email attachments (or configure your gateway anti-virus software to remove this type of attachment).
- Encourage your users to send Microsoft Office documents in formats that cannot contain macros (and therefore cannot be infected with macro viruses), such as .rtf instead of .doc, and .csv instead of .xls.
- Check your email and internet security settings.
- Always use passwords and never disclose them to anyone.
- Keep sound backups of your operating systems, programs and files. Even if you are able to disinfect programs, you must subsequently replace them from backups. Clean boot disks are sometimes necessary to help with disinfection.
- Keep Sophos Anti-Virus up to date at all times.

Installation

About installation

Creating the Windows 95/98/Me CID

Installing Sophos Anti-Virus on the workstations

Testing Sophos Anti-Virus on Windows 95/98/Me

1 About installation

The installation information in this user manual is intended to be used for reference only. It explains all available installation options.

The ***recommended*** installation procedures for Windows 95/98/Me are included in the following installation guides.

- To install Sophos Anti-Virus on a **single Windows 95/98/Me computer**, see the *Sophos Anti-Virus Windows 95/98/Me single user installation guide*. This installation guide also contains information about using and updating Sophos Anti-Virus on a single Windows 95/98/Me workstation.
- To install Sophos Anti-Virus on a **Windows 95/98/Me peer-to-peer network**, see the *Sophos Anti-Virus Windows 95/98/Me peer-to-peer network installation guide*.
- To install Sophos Anti-Virus on networked Windows 95/98/Me workstations **connected to a Windows NT server**, see the *Sophos Anti-Virus Windows NT server installation guide*.
- To install Sophos Anti-Virus on networked Windows 95/98/Me workstations **connected to a Windows 2000 server**, see the *Sophos Anti-Virus Windows 2000 server installation guide*.
- To install Sophos Anti-Virus on networked Windows 95/98/Me workstations **connected to a NetWare server**, see the *Sophos Anti-Virus NetWare server installation guide*.
- To install Sophos Anti-Virus on networked Windows 95/98/Me workstations **connected to a Unix server**, see the *Sophos Anti-Virus Unix server installation guide*.

1.1 System requirements

- At least 8 MB of RAM.
- At least 10 MB of hard disk space.

1.2 The installation process

To install Sophos Anti-Virus on Windows 95/98/Me workstations you

- create a central installation directory (CID) (section 2).
- install Sophos Anti-Virus from the CID onto the workstations (section 3).

2 Creating the Windows 95/98/Me CID

This chapter describes how to create a central installation directory (CID) for Windows 95/98/Me networked workstations.

You must uninstall any other anti-virus software before installing Sophos Anti-Virus.

Creating the CID involves two steps:

- Create the CID (section 2.1).
- Add the latest virus identity files (IDEs) to the CID (section 2.2).

2.1 Create the CID

The **central installation directory** (CID) is the central copy of Sophos Anti-Virus files from which Sophos Anti-Virus is installed on the Windows 95/98/Me workstations. Whenever you update the central installation directory, Sophos Anti-Virus will be updated on the workstations without affecting users.

The options in this section determine how Sophos Anti-Virus will behave on all Windows 95/98/Me workstations on which it is installed in section 3.

The CID can be created from a Windows 95/98/Me workstation or from a Windows NT/2000 file server as follows.

1. Log on with Administrator rights to the server.

   If you have already downloaded and unzipped the Sophos Anti-Virus for Windows 95/98/Me files from the Sophos website, go to step 4.

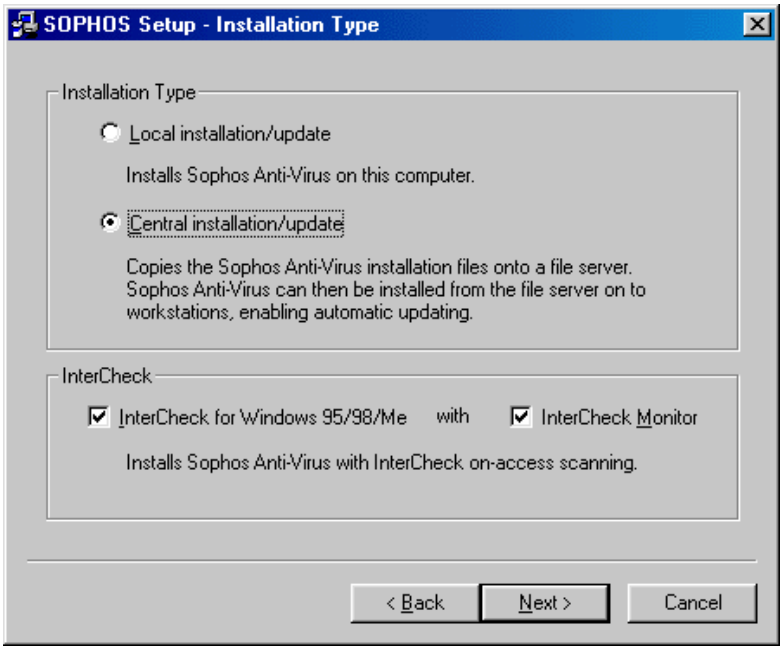
2. Insert the Sophos CD in the CD drive. The CD should auto-run. If auto-run is disabled, run D:\Launchcd (where D: is the CD drive).

3. In the **Sophos CD** window, click **Sophos Anti-Virus**. At the next screen, click **Windows 95/98/Me** and start the setup program.

4. The **SOPHOS Setup** dialog box contains some information about Sophos Anti-Virus.

SOPHOS Setup
sophos anti-virus
SETUP
Sophos Anti-Virus
Sophos Setup will install Sophos Anti-Virus on your system.
To continue with the installation click on Next, otherwise click on Cancel.
< Back
Next >
Cancel

5. In the **SOPHOS Setup - Installation Type** dialog box, confirm that you would like to create a CID, and that you would like to install InterCheck Client on workstations in section 3.


SOPHOS Setup - Installation Type
Installation Type
Local installation/update
Installs Sophos Anti-Virus on this computer.
Central installation/update
Copies the Sophos Anti-Virus installation files onto a file server. Sophos Anti-Virus can then be installed from the file server on to workstations, enabling automatic updating.
InterCheck
InterCheck for Windows 95/98/Me
with
InterCheck Monitor
Installs Sophos Anti-Virus with InterCheck on-access scanning.
< Back
Next >
Cancel

Installation Type

If you click **Central installation/update**, you specify that you would like to create a CID. If you do not click this, a local installation of Sophos Anti-Virus will be made on the computer, which will not update from a CID.

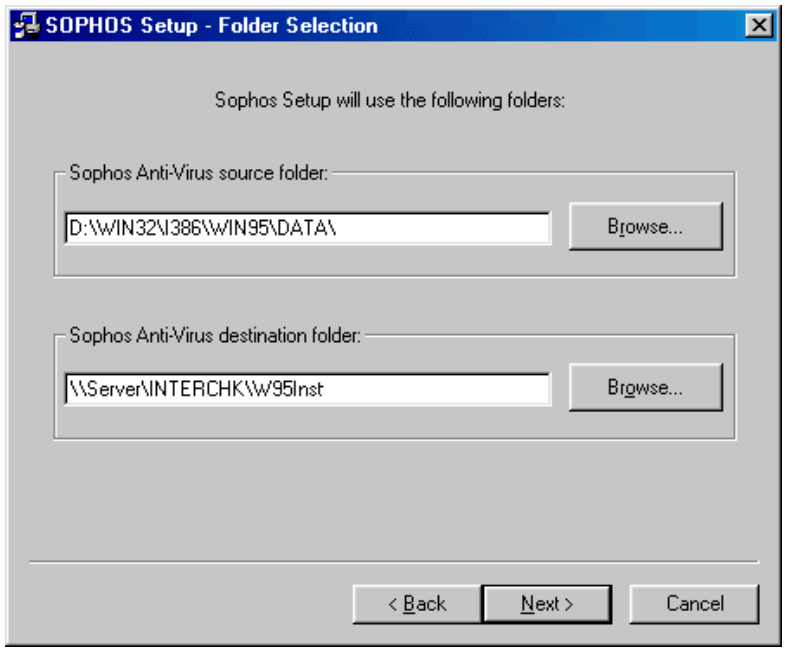
InterCheck

Select **InterCheck for Windows 95/98/Me** to install on-access scanning as part of subsequent local installations.

Select **InterCheck Monitor** if you want to install InterCheck Monitor, an application which confirms that InterCheck is running on a particular workstation. See section 6 for more information.

Both these options are strongly recommended.

6. In the **SOPHOS Setup - Folder Selection** dialog box, confirm the folders **Sophos Anti-Virus** should use.



Sophos Anti-Virus source folder

Do not change this folder.

Sophos Anti-Virus destination folder

The destination folder is the folder on the network drive to which the installation files will be copied. This folder must be visible to users.

It is recommended that this folder is created in the same shared area on the server in which Sophos Anti-Virus for the server platform was installed:

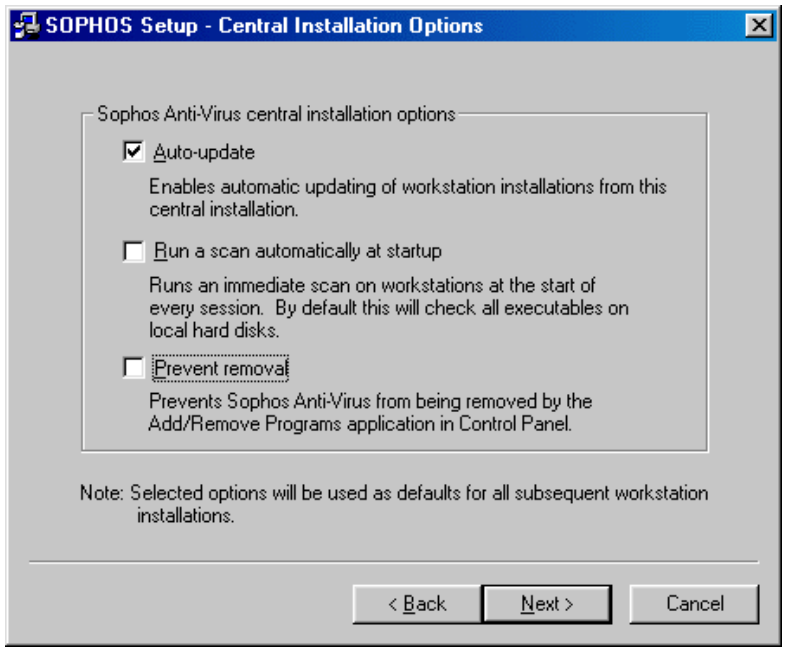
- The Interchk share (on a Windows NT/2000 server).
- The Sophos or InterChk directory (on a Unix server).
- The SYS\SWEEP volume (on a NetWare server).

Click **Browse**, locate the appropriate folder, then double-click it to return to this dialog box. Then type '\W95Inst' at the end of the path.

If you have not yet installed Sophos Anti-Virus on the server, do it before you continue with this procedure (see section 1). If you are installing Sophos Anti-Virus on a peer-to-peer network, see the *Sophos Anti-Virus Windows 95/98/Me peer-to-peer network installation guide*.

When you click **Next**, you may be asked if you would like to create this folder. Click **Yes**.

7. In the **SOPHOS Setup - Central Installation Options** dialog box, choose your installation options.


SOPHOS Setup - Central Installation Options
Sophos Anti-Virus central installation options
Auto-update
Enables automatic updating of workstation installations from this central installation.
Run a scan automatically at startup
Runs an immediate scan on workstations at the start of every session. By default this will check all executables on local hard disks.
Prevent removal
Prevents Sophos Anti-Virus from being removed by the Add/Remove Programs application in Control Panel.
Note: Selected options will be used as defaults for all subsequent workstation installations.
< Back
Next >
Cancel

Auto-update

It is strongly recommended that you select this option. If you do not select it, workstations will not be able to update automatically from the CID when it is updated.

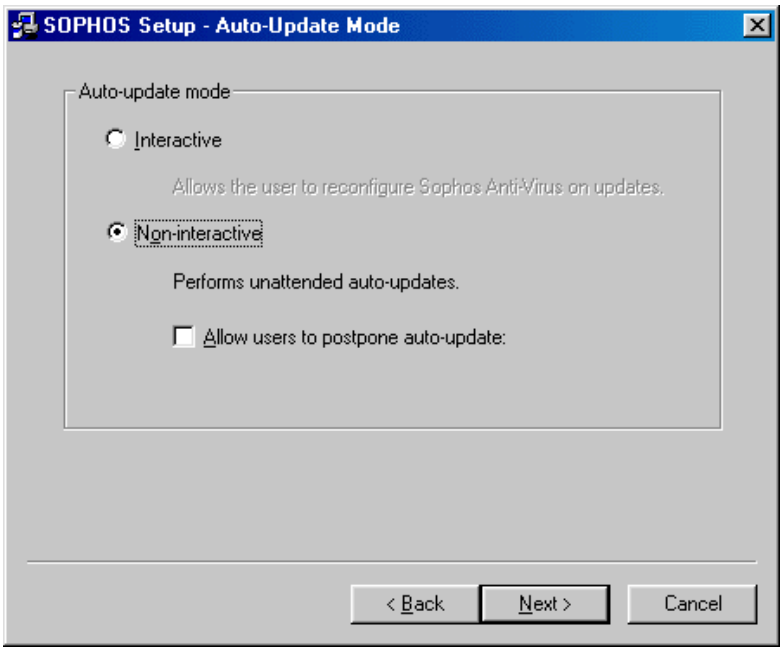
Run a scan automatically at startup

This option is available only if you deselected **InterCheck for Windows 95/98/Me** in step 5. Select this option if you want subsequent workstation installations to run a scan at the start of each session.

Prevent removal

Select this to ensure that subsequent workstation installations cannot be removed via the control panel. This option protects Sophos Anti-Virus from accidental removal.

8. The **SOPHOS Setup - Auto-Update Mode** dialog box is only displayed if you selected **Auto-update** in the previous dialog box.



Interactive

Selecting this option means that during the workstation update process, workstation users will be presented with a number of dialog boxes in which they can configure Sophos Anti-Virus on their own workstation.

Non-interactive

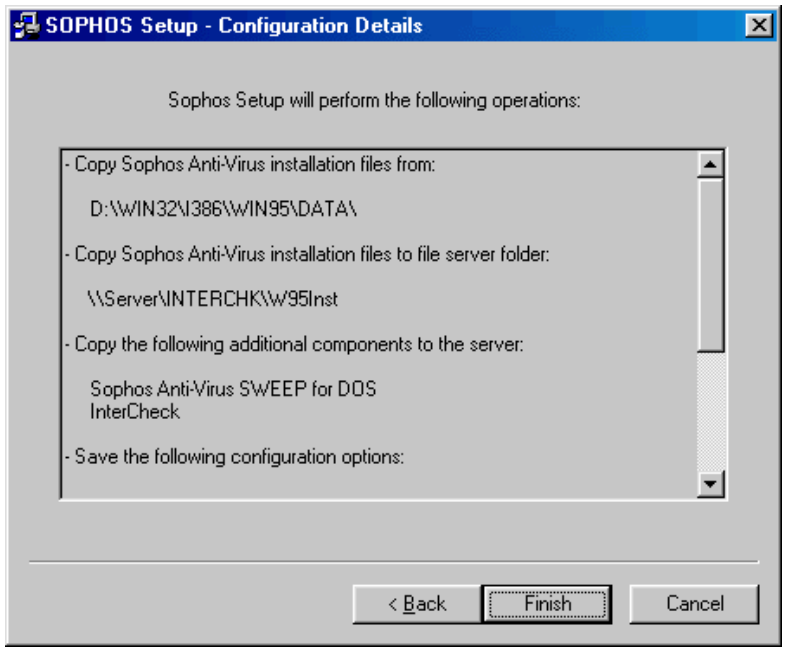
Selecting this option prevents users from reconfiguring Sophos Anti-Virus during updating. They will see only the progress of the update, and can still use their computer during the update. This is the recommended option.

Allow users to postpone auto-update

If you selected **Non-interactive**, this option enables users to postpone the update a specified number of times in a specified period of time. A dialog box is displayed asking the user for confirmation before the update takes place.

This option is only recommended where users connect over a slow link.

9. The **SOPHOS Setup - Configuration Details** dialog box displays your installation options.


SOPHOS Setup - Configuration Details
Sophos Setup will perform the following operations:
- Copy Sophos Anti-Virus installation files from:
D:\WIN32\I386\WIN95\DATA\
- Copy Sophos Anti-Virus installation files to file server folder:
\\Server\INTERCHK\W95Inst
- Copy the following additional components to the server:
Sophos Anti-Virus SWEEP for DOS
InterCheck
- Save the following configuration options:
< Back
Finish
Cancel

10. In the **SOPHOS Setup Complete** message box, click **OK**.

SOPHOS Setup Complete
sophos anti-virus
Sophos Anti-Virus central installation complete.
SETUP location:
\\Server\INTERCHK\W95Inst\SETUP.EXE
You can now run Sophos Setup from the above location to install Sophos Anti-Virus on your workstations.
OK

Now download the latest IDEs from the Sophos website (section 2.2).

2.2 Add the latest virus identity files (IDEs) to the CID

This section describes how to download IDEs from the Sophos website.

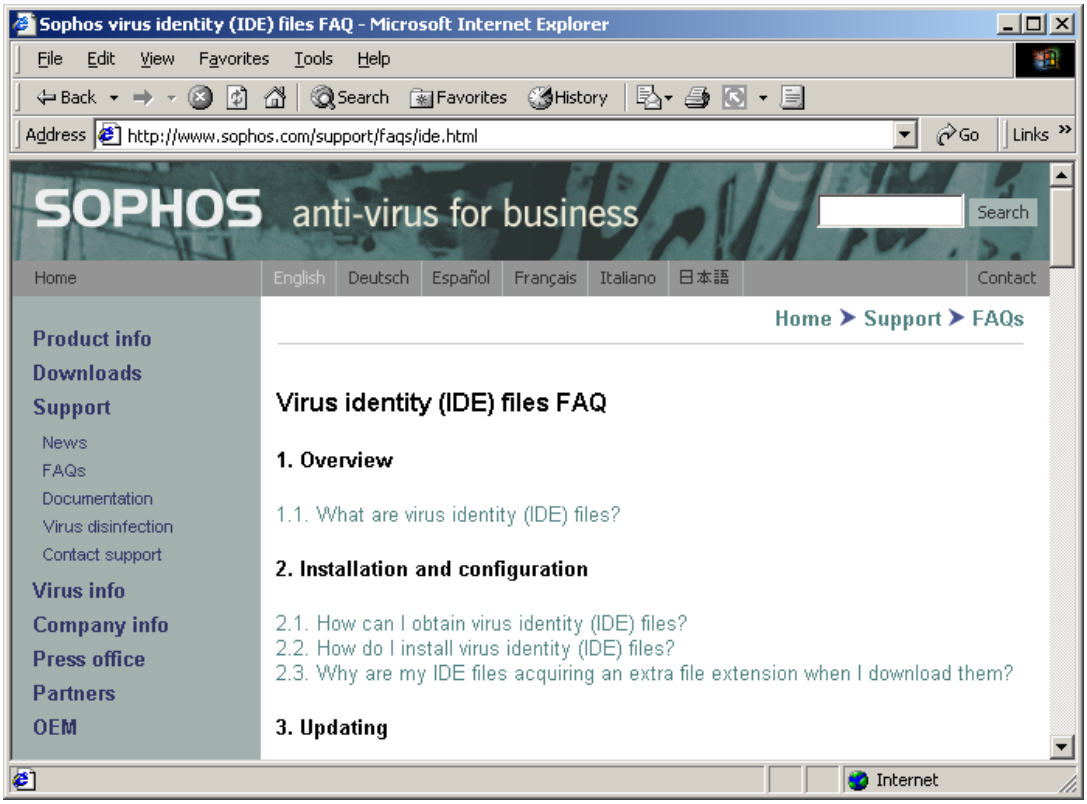
A **virus identity file (IDE)** enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your network against viruses discovered since your version of Sophos Anti-Virus was compiled.

Download IDEs as follows:

1. At the server, go to the IDE download page of the Sophos website (www.sophos.com/downloads/ide).
2. Download the compressed IDEs file for your version of Sophos Anti-Virus.
3. Extract the IDEs to the W95Inst folder in the CID.

If you prefer, scroll down the page and download the IDEs one by one, to the location above.

Help with downloading IDEs is available on the IDE FAQ page of the Sophos website (www.sophos.com/support/faqs/ide.html). If you use Internet Explorer 5.0, read the note on why IDEs may acquire an extra file extension when you download them.



If you need further help with downloading IDEs, please contact Sophos technical support.

Now install Sophos Anti-Virus on the workstations (section 3).

3 Installing Sophos Anti-Virus on the workstations

You can choose one of two different methods to install Sophos Anti-Virus on the Windows 95/98/Me workstations:

- Use the login script to install Sophos Anti-Virus on all Windows 95/98/Me workstations simultaneously, as described in section 3.1.

or

- Install Sophos Anti-Virus on workstations one at a time, by repeating the procedure described in section 3.2 on each workstation.

The first method is more complicated, but saves time on larger networks.

3.1 To install Sophos Anti-Virus using the login script

If you do not already have a login script, refer to your server platform documentation to find out how to create one.

First move the SAVAgent utility to the CID. This will enable SAVAdmin to monitor Sophos Anti-Virus on Windows 95/98/Me workstations after the login script executes.

SAVAdmin is a utility that enables monitoring of Sophos Anti-Virus installations and updates on the network. It is used during installation of Sophos Anti-Virus on Windows NT/2000/XP.

If you have not installed SAVAdmin on a Windows NT/2000 computer on the network (e.g. during installation of Sophos Anti-Virus for Windows NT/2000/XP), go straight to step 6. For more information about SAVAdmin and SAVAgent, see the *SAVAdmin installation guide* or *user manual*.

1. At the Windows NT/2000 computer on which you installed SAVAdmin, right-click the **Start** button to display a menu and select **Explore** to open Windows Explorer.
2. In Windows Explorer, locate

   C:\Program Files\Sophos\SAVAdmin\Ver 2.20

   and double-click it. Single-click Savagent.exe.
3. On the **Edit** menu, click **Copy**.
4. In Network Neighborhood (Windows 95/98) or My Network Places (Windows Me), locate the Windows 95/98/Me CID on the server. For example

   \\[servername]\InterChk

where [servername] is the name of a Windows NT/2000 server.

Open the shared folder.

5. On the **Edit** menu, click **Paste**.

   The file is copied to the shared folder. Make a note of the location of the file.

6. Add the following text to the login script:

   ```
   \\[servername]\...\W95Inst\Setup.exe -inl -a

   start /wait \\[servername]\...\Savagent.exe -update -poll=3600
   ```

   where [servername] is the name of the server on which you created the CID, and [...] is the path to the W95Inst folder in the CID.

   The second line of the script should contain the path to the location of SAVAgent determined in step 5. If SAVAdmin is not installed anywhere on your network, do not include the second line in the login script.

You can leave these lines in the script. They have no effect on computers that already have an installation but automatically install Sophos Anti-Virus on any new Windows 95/98/Me workstations that join the network.

The qualifiers are defined as follows:

–inl	Prevents the Sophos splash screen being displayed during installation or updating on workstations.
–a	Ensures installation and updating happen without users being shown setup dialog boxes that would enable them to configure Sophos Anti-Virus. Instead, settings you input when creating the CID are used.
–update	Ensures that SAVAgent is updated on the workstation whenever a new version is added to the InterChk share. New versions of SAVAgent usually only become available when SAVAdmin is updated (for more information on SAVAgent see the *SAVAdmin user manual*).
–poll=xxx	Sets the auto-update check frequency in seconds (i.e. poll=3600 configures the Windows 95/98/Me workstations to poll for Sophos Anti-Virus updates every sixty minutes).

You can also add the following qualifier to the second line:

–serv	Configures SAVAgent to run in service mode, remaining active when users log off.

The next time users log in, installation takes place and they see InterCheck scanning their workstations.

Installation is complete.

3.2 To install Sophos Anti-Virus without using the login script

First, if you haven't already done so, move the SAVAgent utility to the CID. This will enable SAVAdmin to monitor Sophos Anti-Virus on the Windows 95/98/Me workstation after installation.

SAVAdmin is a utility that enables monitoring of Sophos Anti-Virus installations and updates on the network. It is used during installation of Sophos Anti-Virus on Windows NT/2000/XP.

If you have not installed SAVAdmin on a Windows NT/2000 computer on the network (e.g. during installation of Sophos Anti-Virus for Windows NT/2000/XP), go straight to step 6. For more information about SAVAdmin and SAVAgent, see the *SAVAdmin installation guide* or *user manual*.

1. At the workstation on which you installed SAVAdmin, right-click the **Start** button to display a menu and select **Explore** to open Windows Explorer.
2. In Windows Explorer, locate

   C:\Program Files\Sophos\SAVAdmin\Ver 2.20

   and double-click it. Single-click Savagent.exe.
3. On the **Edit** menu, click **Copy**.
4. In Network Neighborhood (Windows 95/98) or My Network Places (Windows Me), locate the Windows 95/98/Me CID on the server. For example

   \\[servername]\InterChk

   where [servername] is the name of a Windows NT/2000 server.

   Open the shared folder.
5. On the **Edit** menu, click **Paste**.

   The file is copied to the shared folder. Make a note of the location of the file.
6. At the Windows 95/98/Me workstation on which you wish to install Sophos Anti-Virus log on with Administrator rights to the server.
7. At the taskbar, click **Start**|**Run**.

8. In the **Run** dialog box, click **Browse**. Locate and double-click Setup.exe in the W95Inst folder in the CID.

9. In the **Run** dialog box, type '-inl -a' at the end of the path (leaving a space between the path and the new text). Click **OK**.

   The Sophos Anti-Virus files are copied onto the workstation. When they have been copied, Sophos Anti-Virus warns you that the workstation will restart. When the workstation restarts, InterCheck scans the workstation.

   Now, if you carried out steps 1–5, install SAVAgent on the workstation and enable frequent auto-updating:

10. Log back on to the workstation with Administrator rights to the server.

11. At the taskbar, click **Start**|**Run**.

12. In the **Run** dialog box, click **Browse**. Locate and double-click Savagent.exe in the CID.

13. In the **Run** dialog box, type ' -update -poll=3600' at the end of the path (leaving a space between the path and the new text). Click **OK**.

    SAVAgent is installed on the workstation, enabling SAVAdmin to monitor the Sophos Anti-Virus installation on the workstation.

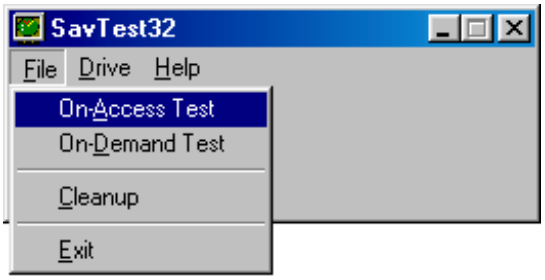
    In addition, the workstation will now check for updates in the CID every hour (3600 seconds), as well as at startup.

    For more information about SAVAdmin and SAVAgent, see the *SAVAdmin user manual*.

4 Testing Sophos Anti-Virus on Windows 95/98/Me

Test the InterCheck Client component of Sophos Anti-Virus as follows.

1. At one of the Windows 95/98/Me workstations, insert the Sophos CD.
2. Right click the **Start** button to display a menu. Select **Explore** to open Windows Explorer.
3. Browse to the Tools\Utils folder and double-click SavTst32.exe.
4. In the **SavTest32** window, on the **File** menu, click **On-Access Test**.



SavTest32 creates a harmless file called EICAR that simulates a virus. Sophos Anti-Virus reports a virus find, and confirms that on-access detection/prevention is working.

On-access detection/prevention is also known as InterCheck.

If SavTest32 reports that on-access detection/prevention is ***not*** functioning correctly, contact Sophos technical support.

When you exit from SavTest32, the test file is deleted.

You can test immediate scanning by clicking **On-Demand** test on the **File** menu. SavTest32 will prompt you to open the Sophos Anti-Virus window and run an immediate scan (see section 5.2).

If InterCheck is running, it will detect the file immediately. Click **OK**.

After the scan, on the **File** menu, click **Cleanup**.

Using Sophos Anti-Virus

Using the Sophos Anti-Virus window

Using InterCheck Monitor

Disinfection

On-screen log messages

5 Using the Sophos Anti-Virus window

This section contains the following information about using Sophos Anti-Virus on both standalone and networked workstations.

- Overview of the Sophos Anti-Virus window (section 5.1).
- How to run immediate scans (section 5.2).
- How to schedule scans (section 5.3).
- Information about InterCheck (section 5.4).

5.1 Overview of the Sophos Anti-Virus window

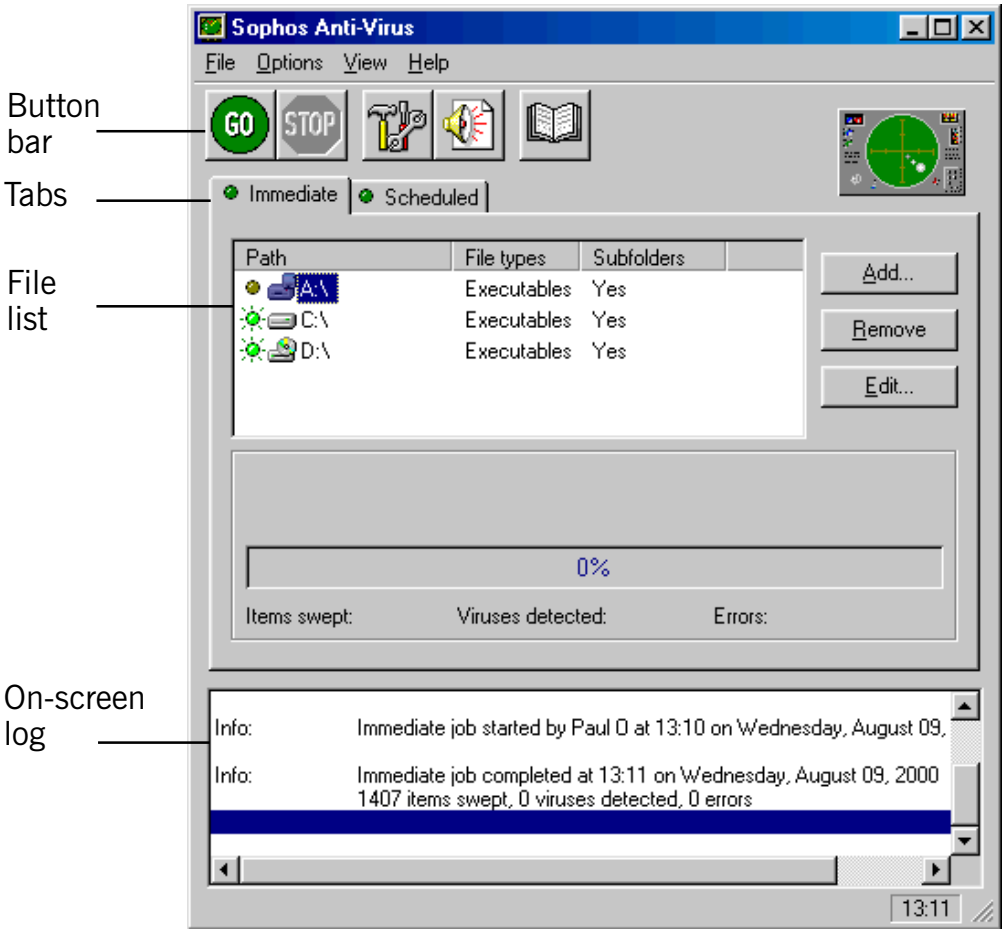
5.1.1 Features of the Sophos Anti-Virus window

This section describes the main features of the **Sophos Anti-Virus** window.

Closing the **Sophos Anti-Virus window** does not stop InterCheck from functioning, although any immediate scans in progress will be terminated.

To start Sophos Anti-Virus, at the taskbar, click **Start|Programs|Sophos Anti-Virus|Sophos Anti-Virus SWEEP**.

The **Sophos Anti-Virus** window is displayed.



Tabs

There is a tabbed page for each type of scan.

Which tabs are available depends on your user status and on whether you view the **Sophos Anti-Virus** window from the server or from a client.

A light on the left of each tab is illuminated when that mode is active or scanning. The tabs are as follows:

- **Immediate** to trigger a scan at any time.
- **Scheduled** for scanning automatically at set times, as long as the computer is switched on.

The button bar

The buttons are shortcuts to commonly-used menu options.

Starts scanning.

Ends scanning.

Opens a dialog box in which you can configure scanning.

Opens a dialog box in which you can configure virus alerts.

Connects you to Virus Info on the Sophos website.

File list

On the **Immediate** tabbed page, the file list shows the drives, paths and files that can be scanned.

On the **Scheduled** tabbed page, the file list is replaced with the scheduled job list. This is a list of the currently active or inactive jobs.

An active light indicates currently selected items. Click on the light to include or exclude items in a scan.

The on-screen log

This contains information about the current session, along with all log messages since Sophos Anti-Virus was started.

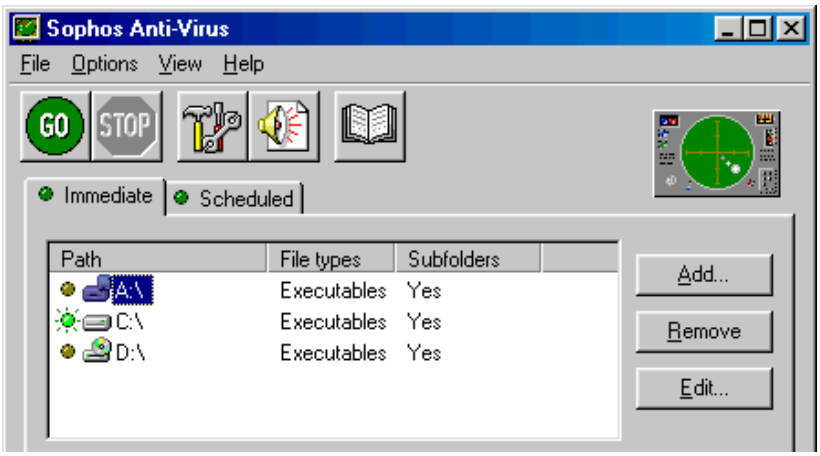
5.1.2 Closing the Sophos Anti-Virus window

To close the **Sophos Anti-Virus** window, on the **File** menu, click **Exit**.

Sophos Anti-Virus may warn you that scheduled scans will not be run if you close down the window. This means that if you want scheduled scans to execute, the **Sophos Anti-Virus** window ***must be open***.

5.2 How to run immediate scans

An **immediate scan** is a virus scan of the computer, or parts of the computer that you can carry out at any time.



The file list shows items that can be included in scans. An illuminated light to the left of an item indicates that it is selected and will be scanned. Click the light to select or deselect items.

5.2.1 Starting an immediate scan

Ensure the **Immediate** tab is selected.

To scan all the selected drives, paths and files, click **GO**.

Alternatively, on the **File** menu, click **Go**.

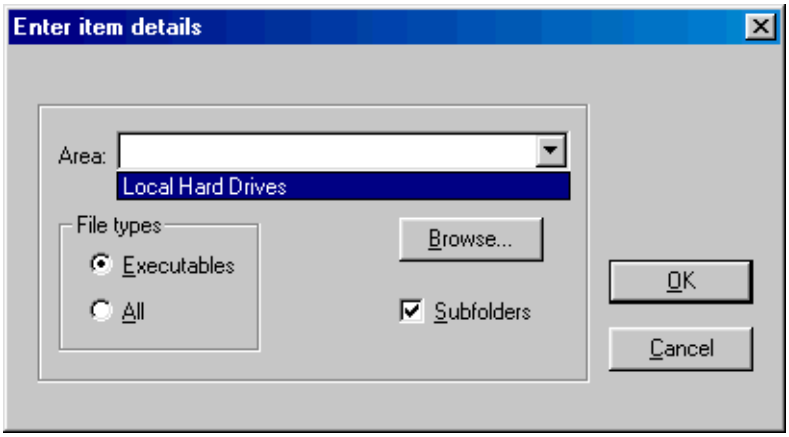
To scan any individual item in the immediate mode display, double-click its icon in the file list.

5.2.2 Default immediate mode file list

By default, all local drives are included in the file list on the **Immediate** tabbed page, and all local hard drives are selected for scanning. You can change the items in the file list as described below.

5.2.3 Adding new items for immediate scanning

To add new items for immediate scanning, click **Add**. The **Enter item details** dialog box is displayed.



Area

Specify the drive, folder or file to be scanned. Both mapped and UNC path names can be entered and wildcards can be included. Alternatively, use **Browse** to select from available items, or use the drop-down menu to select all **Local Hard Drives**.

File types

Only files defined as executables will be scanned, unless **All** is selected. See section 12.3 to find out how to change the files defined as executables.

Subfolders

Subfolders are scanned if this option is selected.

5.2.4 Removing or editing items for immediate scanning

To remove an item, click its path name to highlight it. Then click **Remove**.

To edit the details of an item in the file list, highlight its path name and click **Edit**. The **Enter item details** dialog box (described above) is displayed.

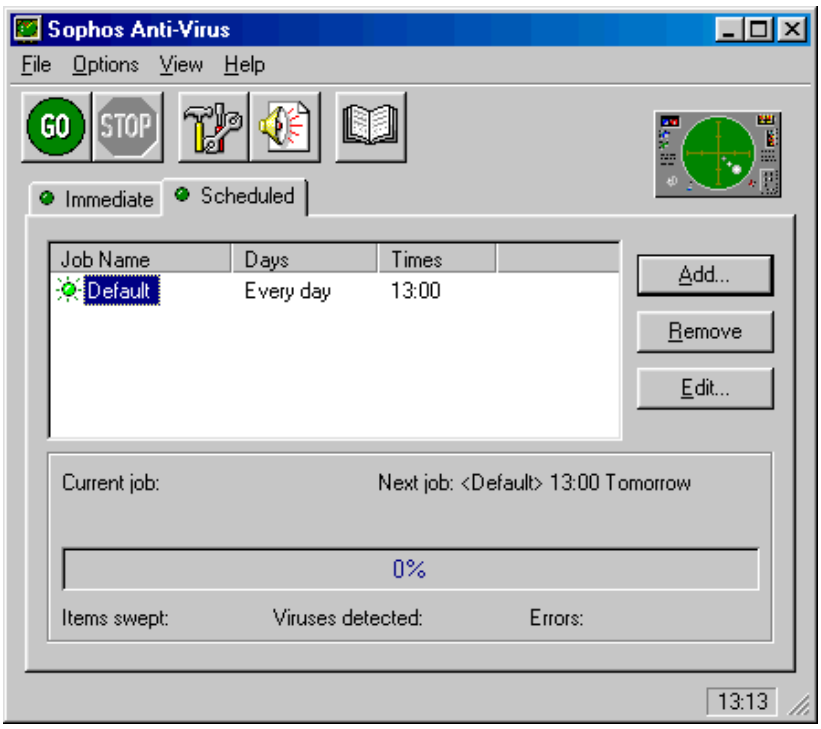
5.3 How to schedule scans

A **scheduled scan** is a scan of the computer or parts of the computer that takes place at a pre-specified time.

A scheduled scan will only execute if the Sophos Anti-Virus window is open at the time the scan is due and throughout the duration of the scan.

To set up a scheduled scan, click the **Scheduled** tab.

The tabbed page lists the available scheduled jobs. An illuminated light to the left of a job indicates that it is selected and will run. Click this light to activate or deactivate jobs.



5.3.1 Default scheduled mode job list

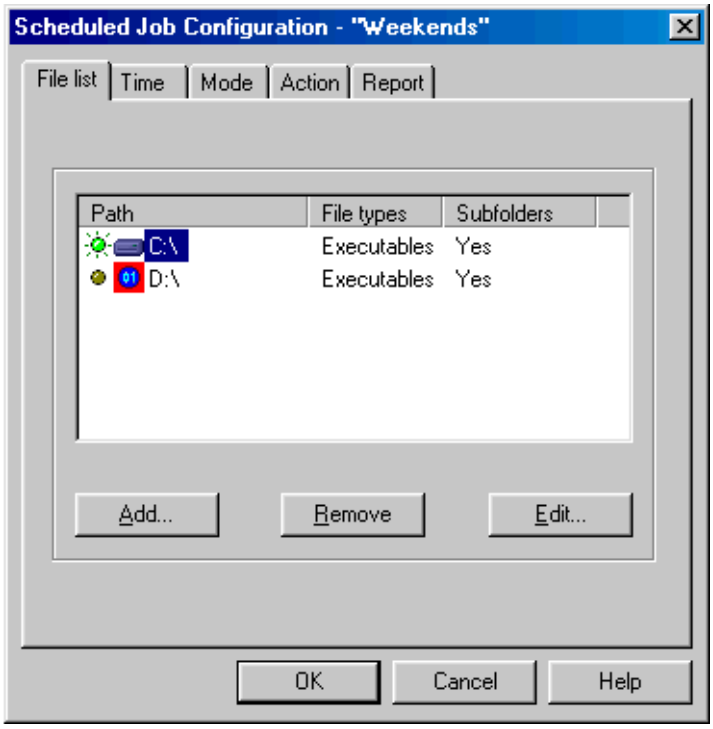
A default job called **Daily** scans the computer at 21.00 every day, as long as it is switched on ***and the Sophos Anti-Virus window is open***.

5.3.2 Adding a new scheduled job

To add a new scheduled job, click **Add** on the **Scheduled** tabbed page.

You are prompted to add a job name. Type a name then click **OK**.

The **Scheduled Job Configuration** dialog box is displayed.



Use the **File list** and **Time** tabbed pages to specify what is scanned and when. For more information about using this dialog box, section 9.4.

5.3.3 Removing a scheduled job

Highlight the name of the job to be removed and click **Remove**.

5.3.4 Editing a scheduled job

Highlight the name of the job you want to edit and click **Edit**. The **Scheduled Job Configuration** dialog box is displayed. For more information about using this dialog box, section 9.4.

5.4 About InterCheck

InterCheck is the on-access scanning component of Sophos Anti-Virus which checks files for viruses every time they are accessed by the computer. If it finds a virus in a file (e.g. in an email attachment), it prevents your computer from opening it.

InterCheck starts automatically each time Windows 95/98/Me is started, before any network connections are made. InterCheck Monitor also becomes active, provided that **InterCheck Monitor** was selected during installation (this is a default setting). See section 6 for information about InterCheck Monitor.

InterCheck for Windows 95/98/Me does not scan archive files. However, it does provide automatic protection against viruses. When an archive is decompressed, InterCheck checks any files that the user attempts to access and denies access if they are infected.

By default, InterCheck for Windows 95/98/Me disables access to floppy disks infected with boot sector viruses.

See section 10 for information about configuring InterCheck.

6 Using InterCheck Monitor

If enabled during installation, the monitor becomes active by default at Windows start up.

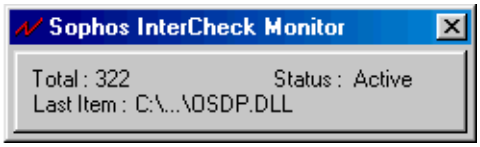
Its function is to confirm that InterCheck Client is active. When it is active, a red lightning flash is displayed in the system tray.

When InterCheck is inactive, the lightning flash is grey.

To start InterCheck Monitor at any other time (i.e. if it has been closed down), at the taskbar, click **Start|Programs|Sophos Anti-Virus|InterCheck Monitor**.

To display InterCheck Monitor, double-click the lightning flash in the system tray.

InterCheck Monitor display



The monitor displays

- the total number of items filtered (i.e. checked against the list of items authorised by InterCheck Client)
- the status of InterCheck Client (active or inactive)
- the name of the last item filtered.

To display the InterCheck Monitor menu, click the left-hand side of its title bar. You can open the **Sophos Anti-Virus** window from this menu.

Closing InterCheck Monitor does not stop InterCheck. As long as the red lightning flash is present in the system tray, InterCheck is active.

7 Disinfection

This section provides some general information about disinfection. ***It does not explain how to disinfect a computer of specific viruses***, as disinfection methods are varied and can be virus-specific.

It is recommended that you get information about the virus (see below), then either use the Sophos website for help with disinfection or contact Sophos technical support.

7.1 Getting information about the virus

If Sophos Anti-Virus reports a virus, first isolate the infected computers from the network and internet.

Write down the name of the virus, then, from an uninfected computer, look up its virus analysis on the Sophos website. The virus analysis search page is located at

www.sophos.com/virusinfo/analyses

The analysis tells you what types of files the virus infects, and provides information about disinfection. It may also include a link to detailed disinfection instructions.

If there are no instructions, or if the virus analysis tells you to seek advice, contact Sophos technical support.

7.2 Disinfection

Sophos Anti-Virus can disinfect many viruses automatically. This includes

- almost all macro viruses
- most boot sector viruses
- some executable file viruses.

To attempt automatic disinfection, enable automatic disinfection for immediate scanning (see section 9.2) then click the **GO** button to run a full scan of the computer.

If the number of viruses reported in the on-screen log decreases, continue running scans until no viruses are found.

If disinfection fails, you should carry out a manual disinfection, specific to that virus and Windows 95/98/Me. This is described on the Sophos website, either in its virus analysis, or on the web page that describes how to disinfect that ***type*** of virus.

7.2.1 If the virus has infected a document

Sometimes you can manually edit the macros from infected documents.

However, contact Sophos technical support before attempting manual disinfection of a macro virus.

7.2.2 If the virus has infected a program

It is impossible to guarantee executable files will be fully restored after disinfection. Restored files may be unstable and put valuable data at risk. You should therefore delete then replace infected programs.

Make a note of the name of the infected executable file/s. Reboot the computer with a clean startup disk (see section 7.3). Locate all the infected executables, delete them, then restore clean versions from the original installation disks, from a clean computer, or from sound backups.

7.2.3 If the virus has infected a boot sector on a floppy disk

Reboot the computer with a startup disk. Then copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the computer has been booted from a startup disk), and reformat the floppy disk.

7.2.4 If the virus has infected a boot sector on the hard disk

Before carrying out this procedure, it is advisable to back up important data on the hard disk.

An infected boot sector on the hard disk should be disinfected. If this is not possible, the boot sector should be replaced with a clean one.

You will need a clean boot disk for the infected computer's operating system (or a startup disk for Windows Me) and a set of Sophos Anti-Virus emergency floppy disks.

See section 7.3 to find out how to create a startup or clean boot disk, and section 7.4 to find out about making Sophos Anti-Virus floppy disk sets.

To disinfect a boot sector

1. Insert the startup disk in the disk drive and restart the computer.
2. If using Windows Me, press 'Ctrl' + 'F5' when the computer restarts.
3. Insert the first emergency disk. Change to the A: drive and run Sophos Anti-Virus for DOS/Windows 3.1x by entering

```
A:
SWEEP *:-DIB
```

To replace a boot sector

If you cannot disinfect the boot sector, overwrite it as follows.

1. Insert the startup disk in the disk drive and reboot the computer.
2. If using Windows Me, press 'Ctrl' + 'F5' when the computer restarts.
3. Check that the contents of the infected drive are visible (e.g. by using DIR C:).

If the contents of the infected drive are not visible, contact Sophos technical support.

4. If the directory listing is okay, overwrite the master boot sector with the command

```
FDISK /MBR
```

or overwrite the DOS boot sector with the command

```
SYS C:
```

7.3 How to create a startup disk

Booting your computer with a startup disk enables you to examine it through a 'clean' operating system, which can be essential to the disinfection process.

7.3.1 To create a startup disk for Windows 95/98/Me

The startup disk must be created on a computer with the same operating system and from the same manufacturer as the infected computer.

Some early versions of Windows 95 do not offer the facility to create a startup disk. If this is the case, or if the disk-creation process does not work, go to section 7.3.2 and create a clean boot disk.

You need one clean floppy disk.

1. On a virus-free Windows 95/98/Me computer, at the taskbar, click **Start**|**Settings**|**Control Panel**.
2. In **Control Panel**, click **Add/Remove Programs**.
3. Click the **Startup Disk** tab, then click **Create Disk**. Follow the on-screen instructions, inserting the disk in the floppy disk drive when prompted.
4. Label the disk clearly, write-protect and store it carefully.

7.3.2 To create a clean boot disk (Windows 95/98 only)

If it is necessary for you to create a clean boot disk, use it in place of the startup disk.

A separate disk is required for Windows 95 (and for different versions of Windows 95) and Windows 98. It is vital that the clean boot disk is created on an uninfected machine.

1. Restart the computer in MS-DOS mode, then insert a disk in the disk drive.
2. At the MS-DOS prompt enter

   ```
   FORMAT A: /S
   ```

3. Copy the following files onto the disk:

   HIMEM.SYS, FDISK.EXE, SYS.COM, DEBUG.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and earlier), FORMAT.COM and EDIT.COM.

   HIMEM.SYS is an Extended Memory (XMS) driver which enables Sophos Anti-Virus to use all the computer's memory thereby improving performance.

These files can be found in C:\Windows and C:\Windows\Command.

4. Create a CONFIG.SYS file that contains the following lines:

   ```
   DEVICE=A:\HIMEM.SYS
   DOS=HIGH,UMB
   FILES=20
   BUFFERS=4
   ```

5. Create an AUTOEXEC.BAT that contains the following lines:

   ```
   SET TEMP=C:\
   SET TMP=C:\
   ```

6. Now write-protect the disk (to ensure it cannot become infected with a virus), and label it with the operating system for which it was created.

7.4 How to create Sophos Anti-Virus floppy disk sets

To create a Sophos Anti-Virus floppy disk set do the following.

1. Insert the Sophos CD at any Windows computer.
2. Using Windows Explorer, browse to the CD and open

   ```
   Diskimg\Diskmake.exe
   ```

   This opens the Sophos disk set creation program.
3. From the drop-down menu, select the type of disk set you would like to make (e.g. **Emergency SAV distribution**). On the screens that follow, accept the defaults by clicking **Next**, until you click **Finish**. Label your disks as instructed.
4. Follow the on-screen instructions to create the disks.

   When the process is complete, write-protect the disks and store them carefully.

7.5 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with, others may have such extreme side-effects that you have to restore a hard disk or replace the BIOS in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. You should keep original executables on write-protected disks so that infected programs can easily be replaced. If you did not have them before you were infected, create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

8 On-screen log messages

This chapter describes messages that can appear in the on-screen log.

8.1 Message categories

There are three kinds of message:

- Administrative messages, such as the times that jobs are started and stopped, and information on the number of viruses detected during a job.
- Virus detected messages, which include the virus name, where it was found, and the action taken.
- Error messages, which alert the user to other problems encountered during the job.

This chapter describes the virus-detected messages and the error messages. Administrative messages are self explanatory.

The sections in square brackets in the messages below indicate information that varies.

8.2 Virus detected messages

Double-clicking a virus name connects you to that virus's analysis on the Sophos website.

Virus: [virus name] detected in [location]
[Action]

This message is displayed if a virus is found during an immediate or scheduled scan. The [location] is one of:

[filename]
Drive [drive name]:
Sector [sector number]
Disk [...]
Cylinder [...]
Head [...]
Sector [...]
Memory block at address [8 digit hex address]

The [action] taken depends on the settings on the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see section 9.2), and is one of the following:

No action taken

No action is taken if you have configured Sophos Anti-Virus not to disinfect boot sectors or documents, and not to rename, delete, shred, move or copy any infected files.

File deleted

The file in which the virus was found has been deleted.

File renamed to [filename]

The [filename] is the old name with the file extension changed to a number. For example, if a virus was named VIRUS.EXE it would be renamed to VIRUS.000, or VIRUS.001 if there was already a file called VIRUS.000.

File shredded

The infected file has been deleted and cannot be recovered.

File moved to [new location]

The [new location] is the location specified on the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see section 9.2).

File copied to [new location]

The [new location] is the location specified in the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see section 9.2).

Error [problem]

The [problem] is one of the following:

deleting [file]
renaming to [filename]
shredding [file]
moving to [location]
copying to [location]

The file could not be deleted, renamed, shredded, moved or copied. If the infected file was found on a floppy disk, check that the disk is not write-protected.

The infected file remains unchanged and may be able to infect other disks and files.

Sophos Anti-Virus has automatically disinfected an item. Run an immediate scan to ensure the computer is now virus free (see section 5.2).

Error: Disinfection failed

Sophos Anti-Virus was unable to disinfect a document or boot sector. See the Sophos website for information about disinfecting specific viruses.

The infected item remains unchanged and may be able to infect other disks and files.

Virus fragment: [virus name] detected in [location]
No action taken

The [location] is one of:

[filename]
Drive [drive name]:
Sector [sector number]
Disk [...]
Cylinder [...]
Head [...]
Sector [...]
Memory block at address [8 digit hex address]

Sophos Anti-Virus does not remove virus fragments. See section 16.3.

8.3 Error messages

Error: Could not open [filename]

The file called [filename] was on the list of files to be scanned, but could not be opened for examination. Check that the file is not in use or already open.

Error: Could not read [filename]

The file called [filename] was on the list of files to be scanned, but could not be read. This might indicate that the file or the disk is corrupt.

Error: Sector size of drive [drive] is too large

Sophos Anti-Virus will only currently scan disk sectors of 2KB or less. It is highly unlikely that your machine will ever contain sectors larger than this.

Error: Could not open report file [filename/folder]

The filename and folder of the report file are specified on the **Report** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see section 9.3). Sophos Anti-Virus cannot open the report file if its filename is not valid, or if it does not have sufficient access rights to the folder.

Error: Log file [filename] could not be opened. Log data will not be saved.

You can specify the location of the log file by using the **Set Log Folder** option on the **File** menu in the **Sophos Anti-Virus** window (see section 12.2). Sophos Anti-Virus cannot open the log file if it does not have sufficient access rights to the file or folder.

Error: Could not notify [user]

The [user] is on the notification list but cannot be notified. This may be because the [user] is no longer on the list of recognised Microsoft Exchange users, or because a profile that requires the user to enter a password was used.

Error: Could not initialize mail system

Sophos Anti-Virus checks to see if Microsoft Exchange is installed before allowing access to the notification options. However, there might be some situations in which Sophos Anti-Virus allows access even though Microsoft Mail is not set up correctly (e.g. if the MAPI mail interface is not installed correctly).

Error: Could not login to mail system

If Sophos Anti-Virus cannot log in to the mail system, the profile name may be invalid.

Error: Could not allocate memory for [filename/folder]

Sophos Anti-Virus needs to allocate memory for the report if it is to send it to the users on the notification list. If the report is too big Sophos Anti-Virus will not be able to load it into memory to send it. The report file can become very large if it is configured to list every file it examines (see section 9.3).

Configuration

Configuring immediate and scheduled scanning

Configuring InterCheck

Alerts configuration options

Global configuration options

Sophos Anti-Virus command line qualifiers

9 Configuring immediate and scheduled scanning

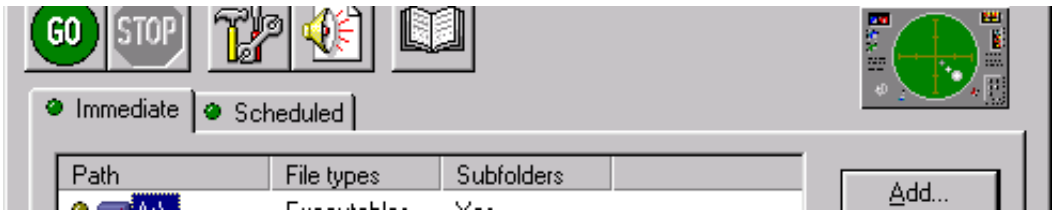
This section describes how to configure immediate and scheduled scanning.

If you want to configure InterCheck (on-access scanning), see section 10.

The different scanning modes are explained in section 5.

Immediate and scheduled scanning each has a configuration dialog box which contains tabbed pages in which you specify which items each mode scans and what action it takes on finding a virus.

To open the required configuration dialog box, in the **Sophos Anti-Virus** window, click the tab for the scanning mode you would like to configure.

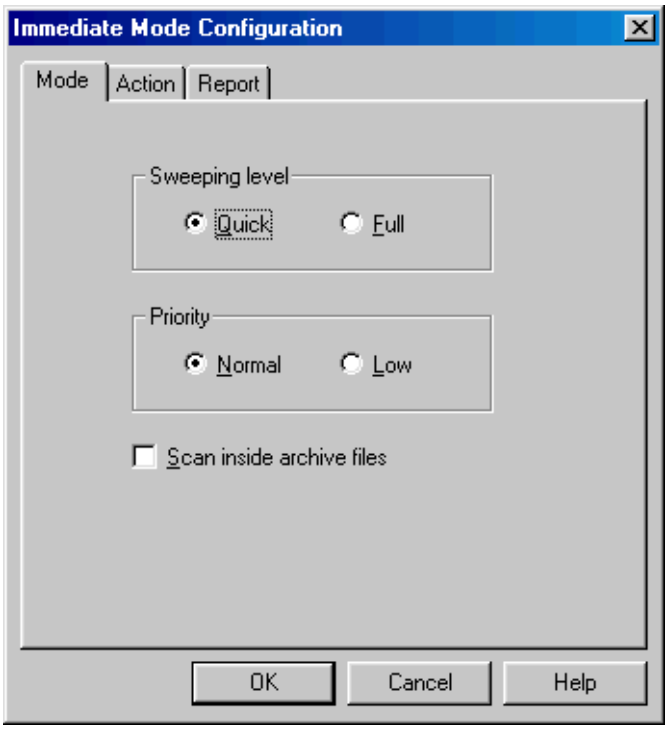


Then click the **Configuration** button.

The sub-sections in this section describe each tabbed page you will find in the configuration dialog boxes.Some tabbed pages are only available for one type of scan.

9.1 Mode

The **Mode** tabbed page enables you to configure scanning activity for both immediate and scheduled scanning



Sweeping level

Quick scanning checks only those parts of each file that are likely to contain viruses. This level is sufficient for normal operation.

Full scanning examines the complete contents of each file. This level is more secure but is much slower than **Quick**.

Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).

Priority

Set Sophos Anti-Virus to run at **Low** priority if you want to minimise the impact on system performance. Note that this increases the time Sophos Anti-Virus takes to scan the system.

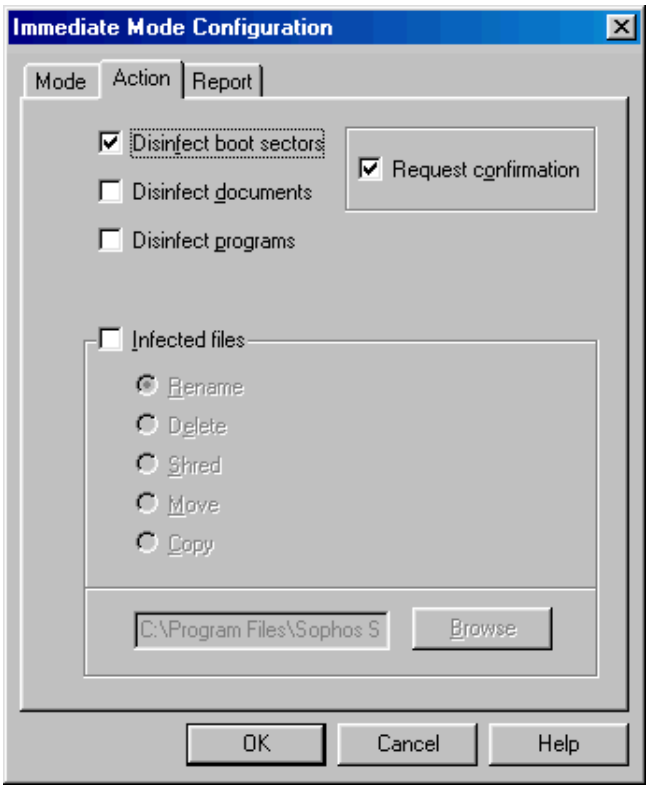
Scan inside archive files

Select this if you want Sophos Anti-Virus to check for viruses inside archive files. Archive types checked include: ZIP, ARJ, RAR, GZIP, TAR, CMZ. You can find a full list of file types scanned by clicking **Executables** on the **Options** menu.

By default, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are also checked.

9.2 Action

The **Action** tabbed page enables you to choose how scheduled and immediate scanning deal with infected items.



Disinfect boot sectors

Sophos Anti-Virus can disinfect most boot sector viruses from floppy disks. It will not automatically disinfect hard disk boot sectors. See section 7 or the Sophos website for information about disinfecting hard disk boot sectors.

Disinfect documents

Sophos Anti-Virus can disinfect documents infected with most types of macro virus. If disinfection fails, the infected file is dealt with in the same way as any other infected file (see **Infected files**, below).

Some macro viruses corrupt the infected document. Check disinfected files carefully before using them. Check the virus analysis on the Sophos website to find out how the virus affects documents it infects.

Infected files

Sophos Anti-Virus can make an infected file safe in several ways other than disinfection.

Renaming or moving an executable file reduces the likelihood of it being run. Deleting or shredding the file disposes of it. Shredding is a more secure type of file deletion that overwrites the contents of the file.

If you choose to move or copy files, you can select a folder for infected files from the browser.

Disinfect programs

Sophos Anti-Virus can disinfect programs. However, it is not recommended that you check this option by default. If Sophos Anti-Virus locates a virus in a program, return to this dialog box and check the **Disinfect programs** option, then run an immediate scan. After disinfection, uncheck this option.

You should subsequently replace the program from a clean backup.

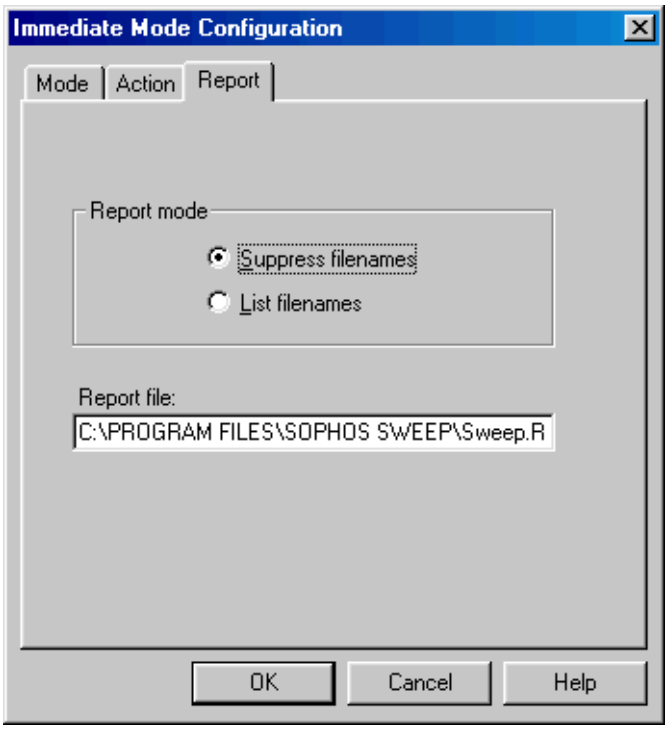
Request confirmation

If you select this option, Sophos Anti-Virus will ask for confirmation before it does anything that involves changing infected items (i.e. disinfection and renaming, deleting, shredding or moving infected files).

This option is available only for immediate scanning.

9.3 Report

The **Report** tabbed page enables you to configure the report file for each immediate or scheduled scan.



Sophos Anti-Virus generates a separate report file for the immediate job and for each scheduled job. This file is provided for the user. It is not the same as the continuous log file.

Report mode

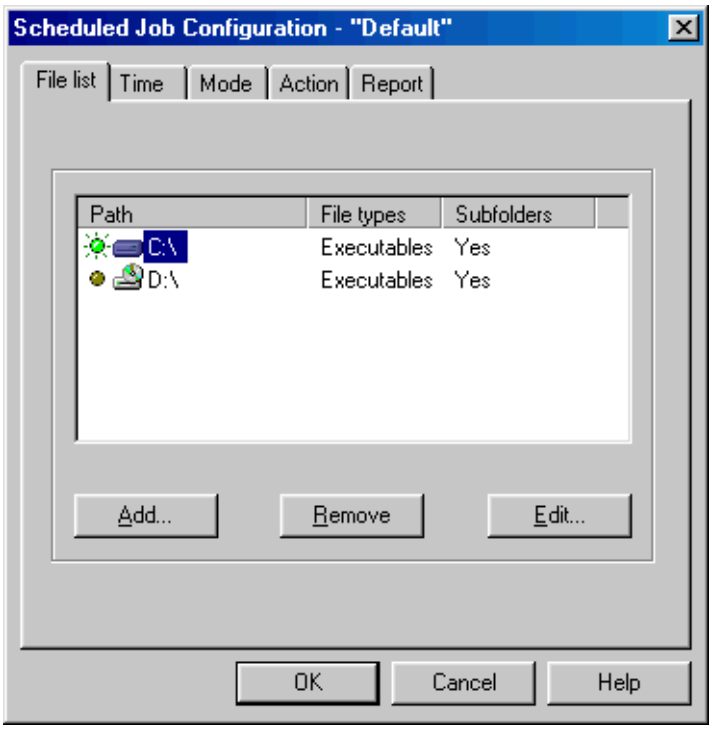
Select **List filenames** if you want Sophos Anti-Virus to record in the report file the name of every item scanned. Otherwise only infected items are recorded.

Report file

Enter a location for the report file or accept the default. This file is deleted and recreated each time the job is run.

9.4 File list (scheduled mode only)

This page enables you to specify what files should be scanned by the scheduled job currently selected in the job list in the **Sophos Anti-Virus** window.

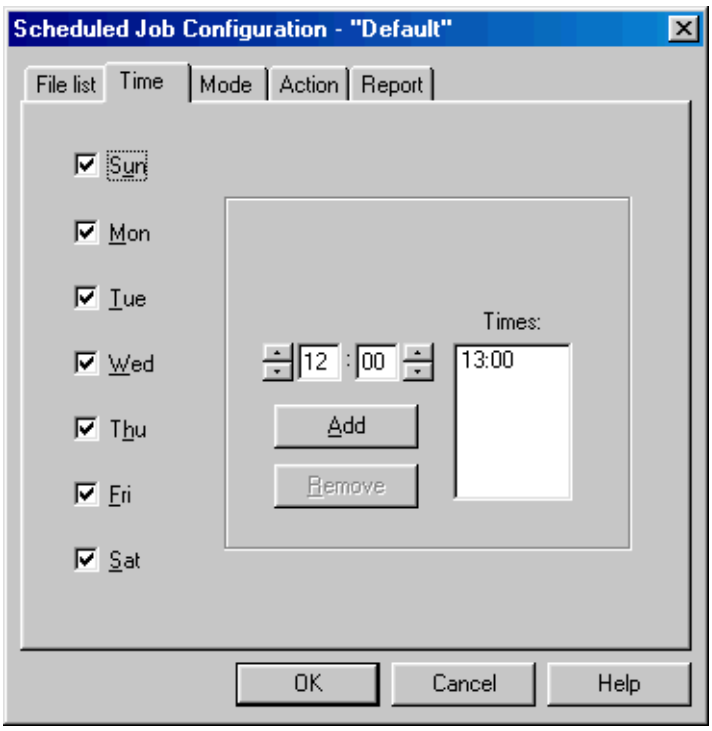


The file list shows drives and files to be scanned by a scheduled job. You can modify the list by using the **Add**, **Remove** and **Edit** buttons.

The default list is the same as that for immediate scanning, except that local floppy disk drives are not listed.

9.5 Time (scheduled mode only)

This page enables you to specify the times at which scheduled jobs will run.



Sophos Anti-Virus can be configured to run at particular times on specific days of the week. By default, a scheduled job is run at 13:00 each day.

Add

To add a time, set the time, click **Add** then click **OK**.

Remove

To remove a time, highlight it, click **Remove** then click **OK**.

10 Configuring InterCheck

This chapter describes how to configure InterCheck (on-access scanning) running on Windows 95/98/Me workstations.

InterCheck (also called InterCheck Client) intercepts files as they are accessed by the user. It uses checksumming to determine whether files have changed since the last time they were last scanned. If they have changed, InterCheck sends them for scanning. If not, InterCheck grants the user access.

This section only describes commonly-used options. For the full list, see the *InterCheck advanced user guide*, available from the Sophos website.

This section contains the following information:

- Is it necessary to configure InterCheck (section 10.1)?
- How is InterCheck configured (section 10.2)?
- Configuring what InterCheck checks (section 10.3).
- Configuring disinfection (section 10.4).
- A list of commonly-used configuration options (section 10.5).

10.1 Is it necessary to configure InterCheck?

InterCheck can be installed and run without making any changes to the default configuration. However, you may wish to

- specify the types of file to be checked
- achieve a balance between initial checking of files and subsequent requests for checking
- configure InterCheck to specify that a file sent for scanning should be disinfected if found to contain a virus.

10.2 How is InterCheck configured?

To configure InterCheck, edit the configuration file Interchk.cfg.

If you installed Sophos Anti-Virus on a standalone computer, edit the Interchk.cfg file in the Sophos SWEEP folder. By default, this folder is located at

C:\Program Files\Sophos SWEEP

If you installed Sophos Anti-Virus on networked computers from a central installation directory (CID), edit the central Interchk.cfg file by default located in

- the Interchk share on a Windows NT/2000 server
- the SWEEP folder in the SYS volume on a NetWare server
- the InterChk or Sophos directory on a Unix server.

When you edit InterChk.cfg in a CID, the changes will take effect on all Windows 95/98/Me workstations the next time they log in.

10.2.1 Editing the configuration file

InterChk.cfg consists of one or more section headers under which you enter configuration options (listed in section 10.4). Here is an example:

```
[InterCheckGlobal]

Exclude=Config.sys

[SweepVxDGlobal]

DisinfectDisks=YES
DisinfectDocuments=YES
```

The section headers indicate different kinds of options, and differentiate options that apply to all workstations from those that apply to specific workstations.

[InterCheckGlobal] applies to all workstations.

[InterCheckWorkStation] applies to specified workstations.

[SweepVxDGlobal] applies to all workstations.

[SweepVxDWorkStation] applies to specified workstations.

Certain options can be used only under the **[SweepVxDGlobal]** or the **[SweepVxDWorkStation]** header. They are indicated in section 10.3.

10.3 Configuring what InterCheck checks

InterCheck sends files for scanning at the following times:

- **At start up**, when a scan is run on the workstation to ensure it is virus-free (see section 10.3.1).
- **During run-time**, when modified items and items that have not previously been checksummed are sent for scanning before they can be accessed (see section 10.3.2).

The levels of checking and scanning at both stages are fully configurable.

10.3.1 Virus scanning at InterCheck start up

InterCheck sends files for scanning

- when InterCheck is first installed and run
- each time the computer is started
- after a Sophos Anti-Virus or IDE update.

The sections below describe each kind of scan and the options used to configure it.

1. Initial InterCheck start up

An initial scan is run after InterCheck is first installed and activated on the computer. This is to check that the system is initially virus-free and to create the initial authorised list of checksums.

The level of scanning at this stage can be set using InstallCheckLevel. The default setting (QUICK) includes all fixed disk boot sectors, memory and files defined as executables.

2. Normal InterCheck start up

This normal, day-to-day start up scan is to detect any memory-resident stealth viruses which, if active when InterCheck loads, may be able to subvert the operation of InterCheck.

LoadCheckLevel can be used to specify what is scanned. The default setting (SYSTEM) includes all fixed disk boot sectors, COMMAND.COM, executables in the root directory, and memory.

3. InterCheck start up after a Sophos Anti-Virus or IDE update

After an update the default level of scanning is the same as that at normal InterCheck startup.

UpdateCheckLevel can be used to specify what is scanned. The default setting is SYSTEM.

Scanning levels at start up

NONE	No scan is performed.
SYSTEM	Memory, boot sectors, COMMAND.COM and hidden system files are scanned.
QUICK	A quick scan of all memory, boot sectors and executables (including COMMAND.COM and hidden system files) on all fixed disks.
FULL	A full scan of memory, boot sectors and executables (including COMMAND.COM and hidden system files) on all fixed disks.
USER	The scan is executed with the command line qualifiers specified by InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions. If the relevant option is not given, the scan executes without any qualifiers.

File types defined as executables

You can change the list of file types treated as executables at each kind of start up. To do this, use InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions to run W95SWEEP with the -EX qualifier and a list of file extensions.

See the *InterCheck advanced user guide* for details.

10.3.2 Virus checking at InterCheck run-time

ProgramExtensions specifies the list of file extensions to be treated by InterCheck as executable files.

The Exclude option specifies files to be excluded from scanning.

10.4 Configuring disinfection

Windows 95/98/Me InterCheck can be configured to disinfect documents containing macro viruses and disks infected with boot sector viruses. To do this, add the following to the configuration file:

```
[InterCheck Global]
SweepVxDLoad=YES

[SweepVxDGlobal]
DisinfectDisks=YES
DisinfectDocuments=YES
```

10.5 Configuration options

DisinfectDisks=YES|NO

If this option is enabled, InterCheck will attempt to disinfect boot sector viruses. By default, it is disabled.

This option is valid only under a SweepVxD header.

DisinfectDocuments=YES|NO

If this option is enabled, InterCheck will attempt to disinfect macro viruses in Microsoft Office files. By default, it is disabled.

This option is valid only under a SweepVxD header.

Exclude=<file>

This option is used to exempt a file from checking. The filename must not include a path component. Up to 32 exclusions may be specified and the '?' character can be used as a wildcard. For example

```
Exclude=PROG?.EXE
Exclude=P2.SYS
```

would suppress the scanning of PROGA.EXE, PROGB.EXE and P2.SYS.

The Exclude configuration option can also be used to disable all checking of a specified drive. For example

```
Exclude=E:
```

would prevent InterCheck from checking anything on the E: drive, including its boot sector.

Note that directories cannot be excluded.

InstallCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

This option defines which files are scanned for viruses when InterCheck is first executed (i.e. installed and then run) on a workstation. The default is QUICK.

See section 10.3.1 for more information.

InstallSweepOptions=<qualifiers>

This option defines the command line qualifiers used when InterCheck is first executed on a workstation. For example, to generate a report as InterCheck is installed, use

```
InstallSweepOptions= -P=C:\INSTALL.REP
```

If InstallCheckLevel is set to NONE, InstallSweepOptions has no effect. If InstallCheckLevel is set to SYSTEM, QUICK or FULL, the scanning options specified by InstallSweepOptions take priority.

LoadCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

This option defines which files are scanned for viruses at normal InterCheck startup. The default is SYSTEM.

See section 10.3.1 for more information.

LoadSweepOptions=<qualifiers>

This option defines the command line qualifiers used at normal InterCheck start up. For example, to generate a report from each workstation as InterCheck is loaded, use

```
LoadSweepOptions=  -P=C:\ICLOAD.REP
```

If LoadCheckLevel is set to NONE, LoadSweepOptions has no effect. If LoadCheckLevel is set to SYSTEM, QUICK or FULL, the scanning options specified by LoadSweepOptions take priority.

PopUpErrorText=<text>

This option defines a text string displayed in the virus alert message box. The default is ‘Please contact the network Administrator immediately’.

The maximum length of the text is 52 characters. Note that word wrapping may be applied to text in the virus alert message box. This can result in fewer than 52 characters being available for use.

ProgramExtensions=<extensions>

Any file whose extension matches an entry in the list of ProgramExtensions is considered by InterCheck to be a program and is checked whenever it is accessed.

If no extensions are given, the default extension list will be used. To see the default list of extensions, open the **Sophos Anti-Virus** window and on the **Options** menu click **Executables**.

The '?' character can be used as a wild card and '.' can be used to represent no extension.

The ProgramExtensions option does not affect checking of files when they are executed, when files are checked irrespective of extension.

See also section 10.3.2.

SweepVxDLoad=YES|NO

This option controls whether or not to use any options defined under a SweepVxD header. When InterCheck is installed locally on Windows 95/98/Me workstations, the installation program automatically adds the option SweepVxDLoad=YES. This should not be changed.

SweepVxDMode=FULL|QUICK

This option controls the level used by InterCheck to scan for viruses. The default is QUICK.

This option may be placed under an InterCheck section header or a SweepVxD section header.

SweepVxDLogFile=<filename>

The SweepVxDLogFile option defines the name of the SWEEPVxD log file. Unless a filename has been defined using this option no information is logged.

This option may be placed under an InterCheck section header or a SweepVxD section header.

SweepVxDLogLevel=0..5

This option controls the amount of information included in the SweepVxD log file.

0 No messages

1 Fatal errors

2 Virus alerts

3 Errors

4 Warnings [Default]

5 Information messages

This option may be placed under an InterCheck section header or a SweepVxD section header.

UpdateCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

The UpdateCheckLevel option defines which files will be scanned for viruses when InterCheck detects a new version of Sophos Anti-Virus. The default is SYSTEM.

See section 10.3.1 for more information.

UpdateSweepOptions=<qualifiers>

The UpdateSweepOptions statement defines the command line qualifiers used when InterCheck detects a new version of Sophos Anti-Virus. For example, to generate a report, use the option:

```
UpdateSweepOptions= -P=C:\ICUPDATE.REP
```

If UpdateCheckLevel is set to NONE, UpdateSweepOptions will have no effect. If UpdateCheckLevel is set to SYSTEM, QUICK or FULL, the scanning options specified by UpdateSweepOptions take priority.

11 Alerts configuration options

This section describes how to configure the alert options available for notifying users about

- scanning activity
- virus finds
- errors.

These options apply to immediate and scheduled scanning only.

These options are configured in the **Notification Configuration** dialog box. To open the dialog box, open the **Sophos Anti-Virus** window and click **Alerts**.

The sub-sections in this section describe the tabbed pages in the **Notification Configuration** dialog box.

11.1 Common options

Each tabbed page shares a number of common features: disable notification, job specification and notification level.

Disable notification

You can turn off the form of notification in the currently-selected tabbed page.

Job specification

If you select **All jobs**, all configuration options selected for that form of notification will apply to immediate mode and all scheduled jobs.

Specific jobs enables you to choose different notification settings for the immediate mode and for each individual scheduled job. If a specific job is not explicitly configured, it inherits the settings of the <default> job.

Notification level

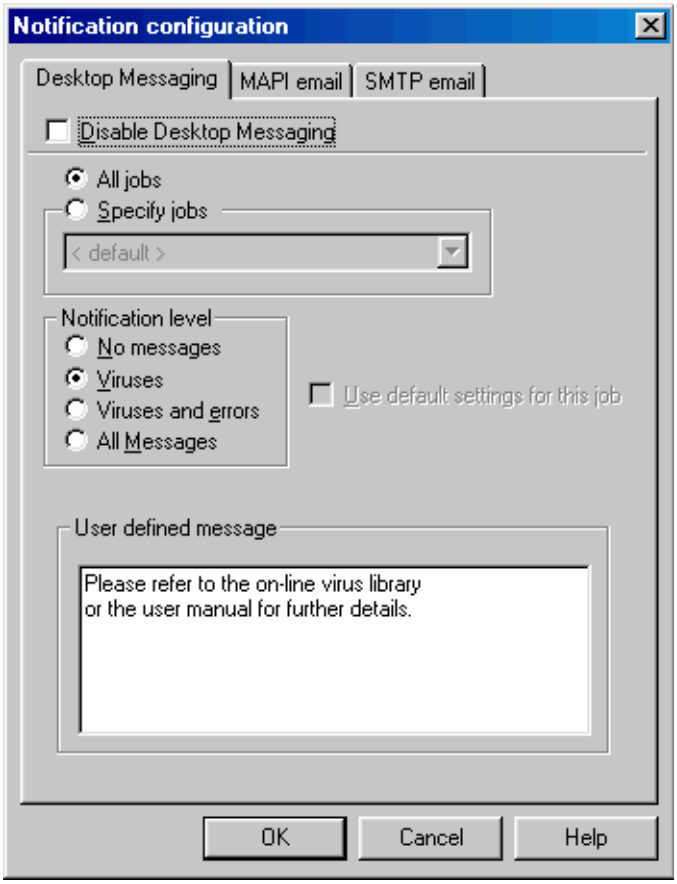
There are four levels of notification to choose from:

- No messages.
- Virus-detected messages only.
- Virus-detected and error messages.
- All messages, including general information, such as the time a job started.

The notification level setting will not affect the level of information placed in the report file, the on-screen log or the log file.

11.2 Desktop messaging

The **Desktop Messaging** tabbed page controls the message displayed when a virus is discovered.

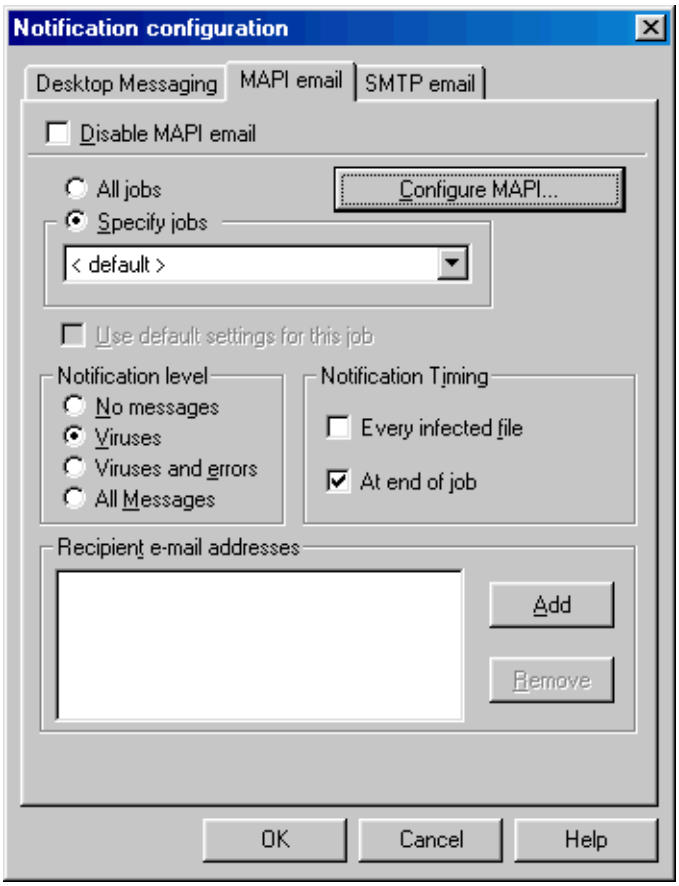


User defined message

The message in this text box is added to the end of the standard virus-detected message.

11.3 MAPI email

The **MAPI email** tabbed page enables you to configure immediate and scheduled scanning to send email notifications on discovery of a virus. This form of notification is only available if Microsoft Exchange is installed.



Recipient e-mail addresses

Add and remove email addresses for the recipients of the notification emails.

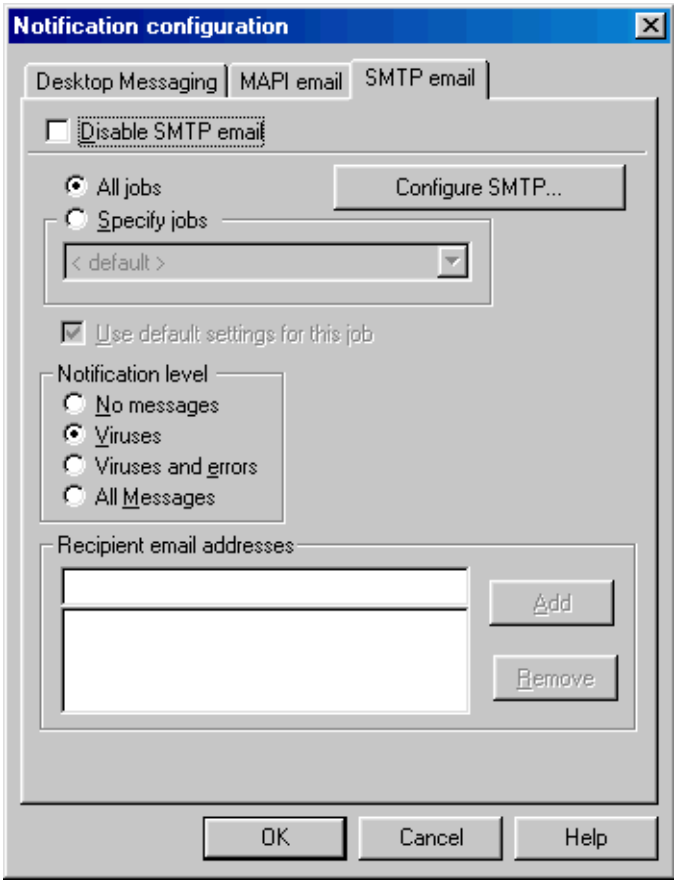
Configure MAPI

To send emails, Sophos Anti-Virus must be able to log on to Exchange without supplying a password. If your default profile requires a password to be entered, do as follows.

1. Click **Configure MAPI**.
2. In the **Set up MAPI profile** dialog box, choose the MAPI profile you want to use.

11.4 SMTP email

The **SMTP email** tabbed page enables you to configure Sophos Anti-Virus to send SMTP email alerts. Mail is sent when a scanning job is completed.



Recipient email addresses

You can add and remove email addresses for the recipients of the messages.

Configure SMTP

It is necessary to enter details of the SMTP server as follows.

1. Click **Configure SMTP**.
2. In the **Set up SMTP** dialog box, under **SMTP server** enter the host name or IP address of the SMTP server.
3. Under **SMTP sender address**, type the email address from which alert emails should appear to originate. Bounces and non-delivery reports will be sent to this address. If no address is entered, no bounces or non-delivery reports will be sent.

12 Global configuration options

This section describes the global configuration options accessible from the menu bar in the **Sophos Anti-Virus** window. It contains the following information:

- How to trigger and immediate scan of memory (section 12.1).
- How to change the location of the Sophos Anti-Virus log folder (section 12.2).
- How to change the files defined as executables for all scanning modes (section 12.3).
- How to exclude files or file types from scanning by all scanning modes (section 12.4).
- How to restore the default configuration (section 12.5).
- How to clear the Sophos Anti-Virus log (section 12.6).
- How to disable the progress bar displayed during a scan (section 12.7).

These options are independent of the scanning mode tabbed pages.

12.1 Sweep memory

Prompts Sophos Anti-Virus to carry out an immediate scan of memory to locate memory-resident viruses.

On the **File** menu, click **Sweep memory**.

Sophos Anti-Virus scans memory for memory-resident viruses automatically when it is first started.

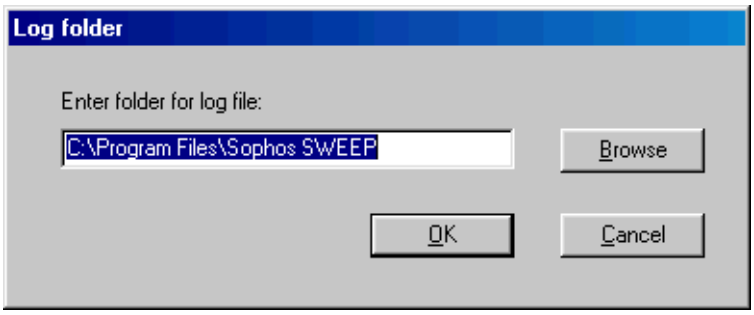
12.2 Set log folder

Enables you to change the location of the log file.

Sophos Anti-Virus maintains a continuous log of all its activity. This log file contains administrative messages along with the on-screen log messages (see section 8). It is generated in addition to the report file, which is aimed at the user (see section 9.3).

By default the log file is saved in the Sophos SWEEP folder, but you can change it as follows.

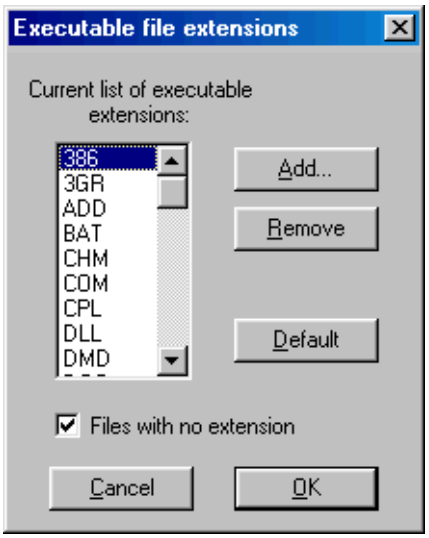
1. In the **Sophos Anti-Virus** window, on the **File** menu, click **Set log folder**.
2. In the **Log folder** dialog box, specify a folder either by typing the path or by using the **Browse** button, and click **OK**.



12.3 Executables

Enables you to configure the types of files scanned when Sophos Anti-Virus is configured to scan executables only.

1. On the **Options** menu, click **Executables**.
2. In the **Executable file extensions** dialog box, specify the file extensions you want to define as executables. Select **Files with no extension** if you also want to include such files.

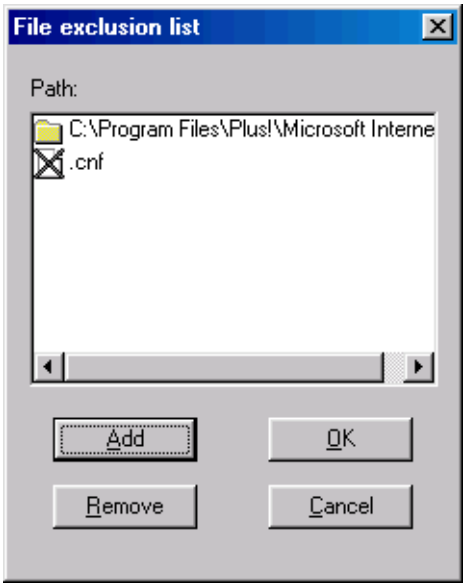


This list is used by Sophos Anti-Virus only if it is set to check **Executables** rather than **All** file types. See section 5.2.3 for more information.

12.4 Exclusion List

Enables you to exclude files from scanning as follows.

1. On the **Options** menu, click **Exclusion List**.
2. To add or remove files from the list, click **Add** or **Remove**. You can also specify file extensions to be excluded from scans.



12.5 Restore defaults

Restores the default settings.

On the **Options** menu, click **Restore Defaults**.

This option destroys all scheduled jobs.

12.6 Clear log

Clears the on-screen log. The on-screen log records information from the current session only. Selecting this option does not clear the continuous log.

On the **Options** menu, click **Clear Log**.

For information about the on-screen log, see section 8.

12.7 Progress bar

Determines whether or not the progress bar is displayed during the type of scanning whose tabbed page is currently selected.

On the **View** menu, click **Progress Bar**.

In order to display the progress bar, Sophos Anti-Virus has to count the items to be scanned before starting. On large network drives this can take a significant amount of time, which is saved by disabling this option. It will not affect any jobs that are already running.

13 Sophos Anti-Virus command line qualifiers

-AUTO Auto start and exit

Starting Sophos Anti-Virus for Windows 95/98/Me from a command line in the following way

```
SWEEP95 -AUTO
```

forces it to perform an immediate scan, with all user-input, stop and unload options disabled.

If no viruses or errors are detected, Sophos Anti-Virus unloads at the end of the job. If viruses or errors are detected, Sophos Anti-Virus displays its normal messages and re-activates all controls.

-I Auto start

Forces Sophos Anti-Virus to perform an immediate scan as soon as it is loaded. User input is not disabled, and Sophos Anti-Virus will not unload at the end of the immediate job.

You can also set Sophos Anti-Virus to start as soon as Windows 95/98/Me starts by placing a shortcut to it in the Windows 95/98/Me StartUp folder.

-NI No interrupting

Suppresses all options to stop Sophos Anti-Virus. The **STOP** button and all internal unload mechanisms are disabled.

When combined with the -I option, all these options are disabled until the end of the immediate job, when they will be re-activated.

-NM No memory check

Suppresses the scanning of memory during Sophos Anti-Virus startup.

-NW No warning messages

Suppresses any warning messages during Sophos Anti-Virus startup. This option is used when Sophos Anti-Virus is installed to start automatically.

Updates

Performing a monthly update

Performing an emergency update

14 Performing a monthly update

Each month a new version of Sophos Anti-Virus is released which includes protection against the latest viruses. Update your network as soon as possible after receiving the new Sophos CD.

Updating involves the following steps:

- Replace out-of-date virus identity files (IDEs) in the central installation directory (CID) with the latest ones from the Sophos website (section 14.1).
- Update the Windows 95/98/Me files in the CID (section 14.2).

If you installed Sophos Anti-Virus using the instructions in this user manual or an installation guide, Windows 95/98/Me workstations will update themselves automatically from the updated CID.

It is possible to fully automate Sophos Anti-Virus for Windows updates using Enterprise Manager. See the Sophos website or contact your local sales office for more information.

More detailed updating information for Windows 95/98/Me workstations is included in the following update guides:

- *Sophos Anti-Virus Windows NT/2000 server update guide.*
- *Sophos Anti-Virus Unix server update guide.*
- *Sophos Anti-Virus NetWare server update guide.*

To find out how to update a single Windows 95/98/Me computer, see the *Sophos Anti-Virus Windows 95/98/Me single user installation guide*.

14.1 Replace the out-of-date IDEs

This section describes how to replace out-of-date IDEs in the CID.

A **virus identity file (IDE)** enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your network against viruses discovered since the latest version of Sophos Anti-Virus was compiled. You must remove out-of-date IDEs before you download the latest ones. For more information, see section 15.1.

Replace IDEs as follows:

1. At the server on which the CID was originally installed, or a workstation that has write access to the server as well as internet access, right-click the **Start** button to display a menu and select **Explore**.
2. In Windows Explorer, locate and open

   \\[servername]\...\W95Inst

   where W95Inst is a folder in the CID on the server. Delete all *.ide and compressed IDEs files in the W95Inst folder.
3. Go to the IDE download page of the Sophos website (www.sophos.com/downloads/ide).
4. Download the compressed IDEs file for the new version of Sophos Anti-Virus.
5. Extract the IDEs to the W95Inst folder.

If you prefer, scroll down the page and download the IDEs one by one, to the location above.

Help with downloading IDEs is available on the IDE FAQ page of the Sophos website (www.sophos.com/support/faqs/ide.html).

If you need further help with downloading IDEs, please contact Sophos technical support.

Now update the Windows 95/98/Me files in the CID (section 14.2).

14.2 Update the Windows 95/98/Me files in the CID

1. Log on to a Windows 95/98/Me workstation with Administrator rights to the server, or carry out the following steps at the server.

   If you have already downloaded and unzipped the Sophos Anti-Virus for Windows 95/98/Me files from the Sophos website, go to step 4.

2. Insert the Sophos CD in the CD drive. The CD should auto-run. If auto-run is disabled, run D:\Launchcd (where D: is the CD drive).

3. In the **Sophos CD** window, click **Sophos Anti-Virus**. At the next screen click **Windows 95/98/Me**, and start the setup program.

4. In the **SOPHOS Setup** dialog box, click **Next** to continue the installation.

5. In the **SOPHOS Setup - Installation Type** dialog box, click **Central installation/update**. Ensure **InterCheck for Windows 95/98/Me** and **InterCheck Monitor** are selected. Click **Next**.

6. In the **SOPHOS Setup - Folder Selection** dialog box, click the lower **Browse** button. Browse to the W95Inst folder in the CID and click it. Click **OK** to return to the **SOPHOS Setup - Folder Selection** dialog box. Click **Next**.

7. In the **SOPHOS Setup - Central Installation Options** dialog box, select **Auto-update** and **Prevent removal**. Click **Next**.

8. In the **SOPHOS Setup - Auto-Update Mode** dialog box, click **Non-interactive**. Click **Next**.

9. In the **SOPHOS Setup - Configuration Details** dialog box, click **Finish** to complete the installation.

10. In the **SOPHOS Setup Complete** dialog box, click **OK**.

    The workstations will update themselves from the CID the next time they are restarted. If you used the -poll qualifier during installation (see section 3), workstations will update themselves in the next hour without needing to be restarted.

15 Performing an emergency update

This type of update is carried out between major monthly updates of Sophos Anti-Virus. Whenever there is a new virus threat, such as a fast-spreading email worm, you should download the virus identity file (IDE) for it from the Sophos website.

This section contains the following information:

- About emergency updating with IDEs (section 15.1).
- Performing a complete emergency update (section 15.2).
- How to set up shortcuts that update the CID automatically after you download a new IDE (section 15.3).

To receive email notifications about IDEs and other alerts, register at www.sophos.com/virusinfo/notifications.

15.1 About updating with IDEs

IDEs enable Sophos Anti-Virus to detect and disinfect new viruses.

They are written using Sophos's proprietary Virus Description Language (VDL) and consist of printable ASCII characters so they can be sent by email or even fax.

IDEs are cross-platform, meaning all different operating system versions of Sophos Anti-Virus can use the same IDE.

You should download IDEs when you install Sophos Anti-Virus, during a monthly update, and whenever a new virus poses a threat to your system. They are not a replacement for full monthly updates of Sophos Anti-Virus.

To check whether or not a workstation is using the IDEs you have downloaded, open the **Sophos Anti-Virus** window on the workstation. The IDEs it is using are listed in the log at the bottom of the window.

If an IDE you downloaded to the CID is not being used by a workstation, check that you followed all the instructions in section 15.2 when you downloaded the IDE.

You should also check that the workstation is configured to update from the CID to which you downloaded the IDE. To find out how to do this, see section 16.2.

15.2 Performing a complete emergency update

1. At a Windows workstation on the network, log on with Administrator rights and go to www.sophos.com/downloads/ide.
2. Scroll down the web page and click the name of the IDE you want to download.
3. Download the file and save it to the W95Inst folder in the CID.
4. At the taskbar, click **Start**|**Run**.
5. In the **Run** dialog box, click the **Browse** button and locate Setup.exe in the W95Inst folder. Double-click it to return to the **Run** dialog box.
6. The path to Setup.exe is shown in the **Open** text box. At the end of the path, type ' -update', leaving a space between the path and the qualifier. Click **OK**.

The **-update** command increments the Sophos Anti-Virus rollout number in the CID, indicating to the workstations that the CID has been updated. If you do not run this command after an emergency update, workstations will not detect the new IDE.

To find out how to set up a shortcut that carries out the -update steps (steps 4–6) automatically, see section 15.3.

It is possible to fully automate Sophos Anti-Virus for Windows updates using Enterprise Manager. See the Sophos website or contact your local sales office for more information.

15.3 Setting up a -update shortcut

This section describes how to set up a shortcut that increments the rollout number in your Windows 95/98/Me CID automatically. The shortcut reduces the time it takes to carry out an emergency update, but is not essential.

The following describes how to set up the shortcut on the desktop. You may instead create a **Start** menu shortcut.

1. At any Windows workstation on the network (e.g. an administrator's workstation), right-click the desktop to display a menu. Select **New**, then **Shortcut**.
2. In the **Create Shortcut** dialog box, click **Browse** and browse to and double-click Setup.exe in the W95Inst folder in the CID.
3. In the **Create Shortcut** dialog box, add the command ' -update' to the end of the path (leaving a space between the path and the qualifier). Click **Next**.
4. Type a name for the shortcut, then click **Finish**.

   From now on, to perform an emergency update, download the IDE, save it to the CID, then double-click the shortcut.

When you carry out a ***monthly*** update, the rollout number is incremented automatically. You do not need to run -update.

Troubleshooting

Troubleshooting

16 Troubleshooting

This section provides answers to some common problems. For more information about error messages in the on-screen log, see section 8.

16.1 Scanning runs slowly

Full scan

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files likely to contain viruses. However, if scanning is set to full, it scans everything, and takes significantly longer to carry out a scan. See section 9.1.

Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).

Checking all files

By default, Sophos Anti-Virus checks only files defined as executables. If it is configured to check all files the process takes longer (see section 5.2.3). If you would like to scan other specific extensions, as well as executable files, add those extensions to the list of extensions Sophos Anti-Virus defines as executables (see section 12.3).

Network drives selected

Network drives may be much larger than a local hard disk, so take significantly longer to scan. Most network interfaces provide much slower access than a local hard disk, which can further slow down the scan.

Progress bar selected

If the progress bar is displayed, Sophos Anti-Virus must count all the items it will scan. This can take several minutes on large network drives. Enable or disable the progress bar by opening the **Sophos Anti-Virus** window and clicking **Progress Bar** on the **View** menu.

16.2 Auto-updating fails to happen

The central installation directory (CID) has not been updated

Ensure you have updated the CID that workstations poll for updates. You can use SAVAdmin to check which CID a computer is polling, as long as Sophos Anti-Virus was installed in such a way as to enable SAVAdmin to access Windows 95/98/Me workstations (see section 3).

In SAVAdmin, locate a workstation that has not auto-updated. Scroll right to the **Central Installation Directory** column. The CID that the computer polls for updates is displayed in the column.

If this CID is not the one you updated, update it now.

Workstations do not update until they are restarted

A Windows 95/98/Me workstation will normally only update from an updated CID the next time it is restarted.

You can configure the workstation to poll the CID for updates during a session by adding the qualifier -poll=x (where x is the polling frequency in seconds) to the login script. See section 3.1.

16.3 Scheduled scans do not run

In Sophos Anti-Virus for Windows 95/98/Me scheduled scans only run if the computer is switched on and the **Sophos Anti-Virus** window is open.

You can configure Sophos Anti-Virus to run scheduled scans when the **Sophos Anti-Virus** window is not open using AT.INI. This is described in the appendix of the *Sophos Anti-Virus DOS/Windows 3.1x user manual*.

16.4 Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are two possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

If a virus fragment is reported, contact Sophos technical support for advice.

16.5 False positives

Sophos Anti-Virus may very occasionally report a virus in a file that is not infected, e.g. if a sequence of bytes in a normal program matches part of a known virus (some polymorphic viruses deliberately include code resembling that in normal programs). If in doubt, contact Sophos technical support for advice.

To decrease the chance of false positives

- only check executables (see section 16.1)
- perform a Quick rather than Full scan (see section 9.1).

16.6 New viruses

Sophos Anti-Virus detects all viruses known at the time it was compiled. It can also detect the very latest viruses by using new virus identity files (IDEs) available from the Sophos website. However, if a new virus has only just appeared, Sophos Anti-Virus may be unable to detect it.

If you suspect that there is an unknown virus on your system, you should

- Visit www.sophos.com and read about the 'Latest Viruses' listed on the home page. You may be able to update Sophos Anti-Virus to detect and disinfect the new virus.
- If you cannot identify your suspected virus in the 'Latest Viruses' list, send a sample and a description of the effects on your system to support@sophos.com.

16.7 Virus not disinfected

If Sophos Anti-Virus has not attempted to disinfect a virus ('No action taken'), check that automatic disinfection is selected (see section 9.2).

If Sophos Anti-Virus could not disinfect the virus, ('Disinfection failed'), it may be that it cannot disinfect that type of virus (see section 7 or contact technical support).

If dealing with a disk or removable media, make sure that it is not write-protected.

Sophos Anti-Virus will not disinfect a virus fragment because it has not found an exact virus match.

See also section 7.

16.8 Sophos Anti-Virus reports errors

After a scan, Sophos Anti-Virus may report that some errors were found. There are two main reasons for errors:

File is corrupt

It can therefore not be scanned by Sophos Anti-Virus.

File is encrypted

If the file contains macros (for example it is a .doc or .xls file), only the main body of the file will have been encrypted (not the macros). You may be warned that the file is encrypted, but the parts of the file that can contain macro viruses will still be scanned.

16.9 Further help needed

On the website at http://www.sophos.com/

Frequently asked questions (FAQs), virus analyses, the latest IDEs, product downloads and technical articles are available on the Sophos website.

By email to support@sophos.com

Include as much information as possible, including operating system and patch level, Sophos Anti-Virus version, how Sophos Anti-Virus has been installed and configured, and the exact text of any error messages.

By telephone on +44 1235 559933

Sophos offers 24-hour, 365-day telephone technical support.

Glossary and index

Glossary

Index

Glossary

Boot sector: The first part of the operating system to be read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.

Boot sector virus: A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Central installation directory: See CID.

Checksum: A value calculated from item(s) of data. InterCheck creates a list of checksums of the files on the computer. If the checksum of a file is found to have changed, it is sent for scanning because it may have become infected with a virus.

CID: Central installation directory; a central location on a network from which Sophos Anti-Virus is installed and updated. You must install a different CID for each platform, and remember to keep every CID up to date.

DOS boot sector: The boot sector which loads the BIOS and DOS into RAM and starts their execution. A common point of attack by boot sector viruses.

Enterprise Manager: A Sophos administration tool that enables automatic downloading of Sophos Anti-Virus for Windows and IDEs from a remote web server to your local CIDs. You can schedule downloads to occur at specified times or trigger downloads on-demand.

Executables: By default Sophos Anti-Virus will check only files it defines as executables (even when full scanning is enabled). It is possible to configure Sophos Anti-Virus to check all files (section 5.2.3), or to change the list of files defined as executables (section 12.3).

Full scan: If configured to full scanning, Sophos Anti-Virus scans all files and all parts of files in the area it has been configured to scan. A full scan takes significantly longer than a quick scan. It is occasionally necessary in order to locate certain viruses. See section 9.1.

IDE: Virus identity file; a type of file that contains the data Sophos Anti-Virus needs to enable it to detect a specific virus. IDEs are issued in between monthly updates to keep Sophos Anti-Virus up to date with the very latest viruses. IDEs should not be used to replace monthly updates.

Immediate scan: A virus scan that is triggered by the user from the Sophos Anti-Virus window. It is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found.

InterCheck/InterCheck Client: A component of Sophos Anti-Virus that intercepts files as they are accessed, and uses checksumming to determine whether or not they should be sent for virus scanning. It can be installed on servers, then switched off if found to affect performance.

InterCheck Server: A component of Sophos Anti-Virus that enables workstations to send virus alerts to a central location.

Macro virus: A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.

Mapped directory: A network drive known by its locally mapped name, e.g. the UNC directory path \\MAIN\USERS\ might be mapped to F:\ on one particular computer on the network.

Master boot sector: The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is switched on (booted). It contains the partition table as well as the code to load and execute the boot sector of the ‘active’ partition.

Memory-resident virus: A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.

NTFS: Windows NT File System.

Polymorphic virus: A self-modifying encrypted virus.

Quick scan: The default scan type. Sophos Anti-Virus scans only the parts of files that can potentially contain executable code.

SAVAdmin: A Sophos administration tool that enables you to copy and paste installations of Sophos Anti-Virus between Windows NT/2000/XP computers on a network, and check they are up to date. See also the *SAVAdmin user manual*.

SAVAgent: A small utility which, when installed on Windows 95/98/Me computers, enables SAVAdmin to monitor them. See also the *SAVAdmin user manual*.

Scheduled scan: A virus scan that is scheduled by the user to take place at a particular time. As with immediate scanning, it is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found. Sophos Anti-Virus for Windows 95/98/Me by default carries out a scheduled scan at 9pm every day, as long as the computer is switched on and the Sophos Anti-Virus window is open.

SMTP: Simple Mail Transport Protocol; the delivery system for Internet email.

SWEEP: A less common term used to describe the component of Sophos Anti-Virus that carries out immediate and scheduled scanning.

SweepVxD: An InterCheck driver file.

Trojan horse: A computer program which carries out hidden and harmful functions. Generally Trojan horses trick the user into running them by claiming to have legitimate functionality. Backdoor Trojans enable other users to take control of your computer over the internet.

UNC: Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL: Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically.

Virus: A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

Virus identity file: See IDE.

Worm: A type of virus that doesn't need a carrier program in order to replicate. Worms replicate themselves then use communications between computers (e.g. email programs) to spread.

Index

A

alert messages
  desktop messaging 66
  disabling 65
  job specification 65
  MAPI email 67
  notification level 65
  SMTP email 68
archive files
  scanning 50
auto-updating 15–24
automatic disinfection 36

B

boot sector
  definition 90
  DOS, replacing 37
  master, replacing 37
boot sector virus
  definition 90
  disinfection 51

C

central installation directory
  creating 11
  definition 90
checksum
  definition 90
CID
  creating 11
  definition 90
compressed files
  scanning 50

D

default settings
  restoring 71
desktop messaging 66
disinfection 35–40, 51
  automatic 36
  boot sector 51
  documents 51
  general information about 6
  removing infected files 52
  unsuccessful 86–87
documents
  disinfection 51
DOS boot sector
  definition 90

E

Enterprise Manager
  definition 90
excluding files from scanning 71
executables
  defining 70
  definition 90
  limiting scanning to 30

F

false positive 86
floppy disk
  disinfecting boot sector 36, 51
full scan 49
  definition 91

H

hard disk
  disinfecting boot sectors 37, 51

I

IDEs
  definition 91
immediate scan
  definition 91
immediate scanning 29–45
  adding items for scanning 30
  level 49
  priority 49
  removing items from scanning 30
  starting 29
infected executables
  dealing with 52
infected files
  removal 52
  shredding 52
InterCheck 33–45
  disinfection 60
  folder selection 14
  virus alert message 61
  what is checked 58–73
InterCheck Client
  definition 91
InterCheck Server
  definition 91
InterCheckGlobal section header 57
InterCheckWorkStation section header 57
INTERCHK.CFG 57
IP address 68

L

log file 53, 65, 69

M

macro virus
  definition 91
MAPI email 67
mapped directory path
  definition 91
master boot sector
  definition 91
  disinfection 37
memory
  scanning 69
memory-resident virus
  definition 92

N

notification level 65
NTFS
  definition 92

O

on-demand scanning 29–45
  removing items from scanning 30
  starting a scan 29
on-screen log 65
  clearing 71

P

polymorphic virus 86
  definition 92
progress bar 72

Q

quick scan 49
  definition 92

R

report file 65

S

SAVAdmin
  definition 92
SAVAgent
  definition 92
scheduled scan
  definition 92
scheduled scanning
  changing a job 32
  default job 31
  file list 54
  level 49
  priority 49
  setting times 55
SMTP email 68
  definition 92
Sophos Anti-Virus
  configuring 48–73
  disinfection 51
  excluding files to be checked 71
  log file 69
  log folder 69
  on-access scanning 33–45
  priority 49
  reporting 53–73
  restoring default settings 71
  scanning archive files 50
  scanning level 49
subfolders
  scanning 30
SWEEP
  definition 92
SWEEP VxD
  log file 62–63
SweepVxD
  definition 93
SweepVxDGlobal section header 57
SweepVxDWorkStation section header 57

T

technical support
  contact information 2
Trojan horse
  definition 93

U

UNC
  definition 93
updating shortcut 81

V

VDL
  definition 93
virus
  definition 93
  disinfection 35–40, 51
  new 86
  polymorphic 86
  recovery from 40
  side-effects 40–45
virus fragment 85
virus identity file
  definition 93

W

worm
  definition 93